

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

DAVID LAU, HAMIDE LAU, K.L. by and through his next friend David Lau, M.L. by and through her next friend David Lau, ALEXANDER LAU, VIVIAN PERRY, HOLLY ABRAHAM, LEROY LAU JR., MICHELLE LEE RAUSCHENBERGER, JAMMIE SMITH, ALEX ROZANSKI, CHRISTOPHER ROSEBROCK, CLARENCE METCALF, KIMBERLY METCALF, STEPHANIE FISHER, THOMAS FOGARTY, C.F. by and through his next friend Stephanie Fisher, K.F. by and through his next friend Stephanie Fisher, JONATHAN CLEARY, APRIL CLEARY, KARYN MARTA, LAWRENCE MARTA, TAYLOR MARTA, THOMAS SCHWALLIE, SARAH SCHWALLIE, SHANNON K. MCNULTY, ABBY KNAPP-MORRIS, K.K. by and through her next friend Abby Knapp-Morris, ERIC LUND, RYAN TIMONEY, DIANE TIMONEY, GREGORY TIMONEY, ANDREA KESSLER, JOSE ALBERTO MORGADO, ERIC MORGADO, ANNA BANZER, SOFIA KESSLER, CONNOR ALEXIAN PLADECK-MORGADO, ADOLF OLIVAS, ERIC HUNTER, KENNA HUNTER, J.H. by and through his next friend Kenna Hunter, K.H. by and through her next friend Kenna Hunter, BETTY BLACK, JOEY HUNTER SR., JOEY HUNTER II, NICHOLAS ROBINSON IV, ERICH ELLIS, JAMES ELLIS, BETHANY WESLEY, MITCHELL STAMBAUGH, CLARENCE WILLIAMS JR., TALISA SHERVON WILLIAMS, SAMANTHA SHERVON WILLIAMS, ABRILL RENEE WILLIAMS, RANDY RISTAU, H.R. by and through her next friend Randy Ristau, SUZANNE RISTAU, CHRISTOPHER POWERS, JONATHAN ASHLEY III, TAMMIE ASHLEY, JONATHAN ASHLEY IV, JORDAN ASHLEY, SONGMI KIETZMANN, BENJAMIN HORSLEY, JOHN HORSLEY, DEBRA PEREZ, ROBIN AKERS, TRACY HERRING, ADAN PEREZ, ANTHONY PEREZ, NICHOLAS PEREZ, BRIAN LAMBKA, JORDAN LAMBKA, KRISTIE SURPRENANT, BOB SURPRENANT, MATT GRIFFIN, SHAWN PATRICK GRIFFIN, SHEILA RISTAINO, DANIEL GRIFFIN, CAROL GRIFFIN, CHARLES ESSEX, MARION RUTH HOPKINS, MARY BORDER, KATHERINE ABREU-BORDER,

JURY TRIAL DEMANDED

Case No.: 22-cv-1855

DELAYNIE K. PEEK, NATALIE SCHMIDT, A.L.S. by and through his next friend Natalie Schmidt, PHILLIP J. SCHMIDT, LEEANN SCHMIDT, BRANDON SCHMIDT, CREIGHTON DAVID OSBORN, KADE OSBORN, KATLYN M. OSBORN, CHRISTA L. OSBORN, CHERYL ATWELL, ERIN RIEDEL, LONA L. BOSLEY, BRITTANY TOWNSEND, KEVIN TRIMBLE, L.C.D by and through his next friend Bridgett L. Dehoff, KIRK GOLLNITZ, TYLER GOLLNITZ, JAN MARIE HURNBLAD SPARKS, GARRY LEE SPARKS, ERIK SPARKS, ZACHARY DOUGLAS SPARKS, JANE SPARKS, JERRY HARDISON, JUSTINA HARDISON, EDWARD KLEIN, PAUL JAYNE, SHERRY SKEENS, ADAM JAYNE, AYZIA JAYNE, KENT SKEENS, GARRETT SKEENS, TRENT SKEENS, Z.S, by and through her next friend Kent Alan Skeens, CASSIE MARIE RICHARDSON, JOHN MEANS, TAMMIE SCHOONHOVEN, A.M.S. by and through her next friend Tammie Schoonhoven, A.R.S. by and through her next friend Tammie Schoonhoven, DEBORAH SCHOONHOVEN, CHRISTOPHER SCHOONHOVEN, SHEESTA PERRY, HELENA DAVIS, C.D. by and through his next friend Helena Davis, COLLEEN WHIPPLE, MARY BETH SMEDINGHOFF, THOMAS SMEDINGHOFF, JOAN M. SMEDINGHOFF, MARK T. SMEDINGHOFF, REGINA C. SMEDINGHOFF, MARIA CARDOZA, RAMIRO CARDOZA SR., RAMIRO CARDOZA JR., MIRANDA LANDRUM, B.R.L. by and through her next friend Miranda Landrum, G.B.L. by and through his next friend Miranda Landrum, JANET LANDRUM, JAMES R. LANDRUM, CHET MURACH, WILLIAM ANTHONY MURACH, CHRISTINE H. PHILLIPS, S.N.P. by and through her next friend Christine H. Phillips, TRACEY M. PRESCOTT, AARON WILLIAM PRESCOTT, JACOB RICHARD PRESCOTT, JOSHUA MICHAEL PRESCOTT, SAMANTHA JEAN MCNAMARA, BRENDA DAEHLING, KIRK DAEHLING, ADAM DAEHLING, KAYLA MARIE DAEHLING, JOANNA GILBERT, JESSICA A. BENSON, LIESELOTTE R. ROLDAN, ANGEL R. ROLDAN, MATTHIAS P. ROLDAN, SAMANTHA G. ROLDAN, NANCY M. MULLEN, MIRIAM A. MULLEN, WILLIAM J. MULLEN, JOELLE RENÉ ELLIS, JOHN F. ELLIS,

JAMES EARL ELLIS, BRANDON KORONA, MICHELLE MARIE ZIMMERMAN, CHRIS LEE ZIMMERMAN, BAILY ZIMMERMAN, BRUCE NICHOLS, M.G.N. by and through her next friend Bruce Nichols, JEANNE NICHOLS, LORRIA WELCH, BARRY WELCH, ZACKARY WELCH, TAMMY OLMSTEAD, WILLIAM MICHAEL BURLEY, MICHAEL COLLINS, DAN OLMSTEAD, MARTHA CAROLINA SMITH, THOMAS ELMER WICKLIFF, MICHELLE CAROLINA ROTELLI, WILLIAM NEVINS, GARRETT LAYNE FUNK, ANGELA KAHLER, NANCY WILSON, ASHLEY PETERS, G.R.P. by and through his next friend Ashley Peters, DEBORAH JEAN PETERS, DENNIS W. PETERS, PATRICIA GOINS, PAUL EDWARD GOINS III, EMMITT DWAYNE BURNS, JANICE CARUSO, DANA RAINEY, KATHLEEN L. ALEXANDER, DANIEL O. HUGHES, PATRICIA S. HUGHES, KRISTINE ANNE ZITNY, JOE TORIAN EMILY TORIAN, ALBERTO DIAZ, KAYLA DIAZ, N.J.D. by and through her next friend Kayla Diaz, N.J.A.D. by and through his next friend Kayla Diaz, FRANCES DIAZ, MAXIMO DIAZ, ANTHONY DIAZ, MATTHEW DIAZ, MICHELLE RILEY, RODNEY RILEY, JULIE K. MARTIN, BRIAN M. MARTIN, CATHERINE G. MARTIN, ELIZABETH A. MARTIN, JEAN S. LANDPHAIR, DOUGLAS A. LANDPHAIR, MEREDITH LANDPHAIR, KELLI DODGE, B.C.D. by and through his next friend Kelli Dodge, P.A.D. by and through her next friend Kelli Dodge, KATHLEEN MCEVOY, MICHELLE ROSE MCEVOY, PATRICK CHARLES MCEVOY, JANICE H. PROCTOR, LUANN VARNEY, HARRIET SUTTON, ERIN GOSS, SUMMER SUTTON, TRECIA BROCK HOOD, WENDY SHEDD, FREDDIE SUTTON, BARBARA A. ROLAND, MARK K. ROLAND, ERICA M. ROLAND, ANNIE L. MCBRIDE, CHESTER R. MCBRIDE SR., ALEXANDRA MCCLINTOCK, D.C.M. by and through his next friend Alexandra McClintock, JOYCE PATRICIA PAULSEN, GEORGE MCCLINTOCK III, KEVIN KING, STEPHANIE MILLER, TIMOTHY BAYS, APRIL BAYS, LINDSAY BAYS, BRENDA GRINER, JASMIN BAYS, JULIA STEINER, L.S., by and through her next friend Jasmin Bays, M.S., by and through her next friend Jasmin Bays, CHRISTOPHER

BALDRIDGE, S.B., by and through her next friend
Christopher Baldridge, L.B., by and through his next
friend Christopher Baldridge, E.B., by and through his
next friend Christopher Baldridge, ANNGEL
NORKIST, AUJZA NORKIST, HART NORKIST,
WILLIAM NEWNHAM,

Plaintiffs,

v.

ZTE CORPORATION, ZTE (USA) INC., ZTE (TX)
INC., HUAWEI TECHNOLOGIES CO., LTD.,
HUAWEI TECHNOLOGIES USA INC., HUAWEI
DEVICE USA INC., FUTUREWEI TECHNOLOGIES,
INC., and SKYCOM TECH CO., LTD.,

Defendants.

**COMPLAINT FOR VIOLATION
OF THE ANTI-TERRORISM ACT**

Ryan R. Sparacino (*pro hac vice*)
Eli J. Kay-Oliphant
(EDNY Bar No. EK8030)
SPARACINO PLLC
1920 L Street, NW, Suite 835
Washington, DC 20036
Tel: 202.629.3530
ryan.sparacino@sparacinopllc.com
eli.kay-oliphant@sparacinopllc.com

TABLE OF CONTENTS

	Page
A. THE ZTE DEFENDANTS	19
B. THE HUAWEI DEFENDANTS	20
I. SINCE THE ISLAMIC REVOLUTION IN 1979, THE ISLAMIC REVOLUTIONARY GUARD CORPS, OR IRGC, HAS FOMENTED AND SUSTAINED ANTI-AMERICAN TERRORISM	24
A. ISLAMIC REVOLUTIONARY GUARD CORPS	25
B. HEZBOLLAH.....	31
C. QODS FORCE.....	36
II. HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC LED A CONSPIRACY TO ACCOMPLISH THEIR “SECURITY” MISSION OF EXPELLING THE UNITED STATES FROM THE MIDDLE EAST AND FULFILL THE IRGC’S CONSTITUTIONAL DUTY TO PROMOTE TERRORISM TO EXPORT THEIR ISLAMIC REVOLUTION.....	40
A. THE OBJECT OF THE CONSPIRACY AND ITS LEADERSHIP	41
B. THE PARTIES TO THE CONSPIRACY: WHEN EACH MEMBER PROVIDED SECURITY AID TO OTHER MEMBERS OF THE CONSPIRACY, SUCH MEMBER DID SO TO AID THE IRAQ TERROR CAMPAIGN AND AFGHANISTAN TERROR CAMPAIGN IN FURTHERANCE OF THE CONSPIRACY.	45
1. FTO/SDGT Co-Conspirators	45
2. Corporate Front Co-Conspirators	45
i. MTN Irancell.....	46
ii. MTN Group.....	46
iii. TCI and MCI.....	48
iv. Exit40	48
3. Corporate Supplier and Manufacturer Co-Conspirators	49
C. PLAINTIFFS WERE INJURED BY ATTACKS IN AFGHANISTAN THAT OCCURRED IN FURTHERANCE OF THE CONSPIRACY	51
1. The Iraq Terror Campaign	52

2.	The Afghanistan Terror Campaign	52
III.	AFTER 9/11, HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, TALIBAN, AND AL-QAEDA JOINED A CONSPIRACY LED BY THE IRGC TO DRIVE THE UNITED STATES OUT OF AFGHANISTAN, IRAQ, AND THE MIDDLE EAST THROUGH ATTACKS SUPPORTED BY COMMON FUNDING SOURCES, TECHNOLOGIES, AND CORPORATE PARTNERS IN ORDER TO SUSTAIN A TERRORIST ALLIANCE THAT COULD COUNTER NATO	54
A.	THE FORMATION OF THE CONSPIRACY	54
1.	After 9/11, Hezbollah, The Qods Force, And Regular IRGC Led A Terrorist Conspiracy Targeting Americans In Afghanistan, Iraq, And Elsewhere To Inflict Pain On “The Great Satan”	54
2.	To Maximize The Lethality Of Their Terrorist Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Provided Material Support To Every Other Member of the Conspiracy, Including Funds, Arms, Training, And Logistical Support, Which Their Co-Conspirators Used To Attack Americans in Afghanistan.....	54
i.	IRGC Shiite Terrorist Proxies.....	56
ii.	IRGC Syndicate Terrorist Proxies	58
B.	IN FURTHERANCE OF THE CONSPIRACY, HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, AND THE MEMBERS OF THE AL-QAEDA-TALIBAN TERRORIST SYNDICATE WAGED A DEADLY TERRORIST CAMPAIGN AGAINST AMERICANS IN AFGHANISTAN	59
1.	Al-Qaeda	63
2.	Sirajuddin Haqqani (Al-Qaeda and Taliban)	73
3.	The Taliban, Including Its Haqqani Network	79
i.	The Taliban	79
ii.	The Haqqani Network.....	82
4.	The Kabul Attack Network.....	86
C.	IN FURTHERANCE OF THE CONSPIRACY, HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC OPERATED AS AN INTEGRATED TRANSNATIONAL TERRORIST ORGANIZATION WITH A COMMON	

DOCTRINE, STRATEGY, FINANCIAL STRUCTURE, LOGISTICS STRUCTURE, AND COMMAND-AND-CONTROL	88
1. The IRGC’s Transnational Terrorist Strategy, Doctrine, And Tactics Emphasizes The Deployment Of Joint Cells Of Terrorists Led By Hezbollah, Funded And Resourced By The Qods Force, And Supported By Local Iranian Terrorist Proxies	88
2. Hezbollah, The Qods Force, And Regular IRGC Follow Common Terrorist Techniques, Tactics, And Procedures And Use The Same Terrorist Tradecraft To Ensure Concealment And Cover Worldwide.....	89
i. Concealment.....	91
ii. Cover.....	95
iii. Slush Funds For “Off-Books” Terrorist Finance	96
iv. Corruption As Terrorist Tactic And Tool	96
v. Required Donations (<i>Khums</i>) From All IRGC Members.....	97
3. Hezbollah’s, The Qods Force’s, And Regular IRGC’s Terrorist Tradecraft And Doctrine Has Historically Relied On Fronts, Operatives, Agents, Cut- Outs, And Orbits To Fund, Arm, And Operationally Aid IRGC Terrorist Proxy Attacks Against Americans	99
D. IN FURTHERANCE OF THE CONSPIRACY, HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC MANAGED A TRANSNATIONAL NETWORK OF TERRORIST FINANCE, LOGISTICS, OPERATIONS, AND COMMUNICATIONS CELLS TO FUND, ARM, LOGISTICALLY SUSTAIN, AND FACILITATE ATTACKS ON AMERICANS IN AFGHANISTAN	102
1. United States	102
2. U.A.E.; Iraq; Iran; Lebanon; Yemen; Syria; Afghanistan; Pakistan.....	104
3. South Africa	105
4. Europe	107
5. The Americas	107
6. Southeast Asia.....	107
IV. THE CONSPIRACY DEPENDED UPON THE CO-CONSPIRATORS’ ROBUST ACCESS TO U.S. TECHNOLOGY, U.S. DOLLARS, AND U.S.	

PERSONS TO CARRY OUT ATTACKS AGAINST AMERICANS IN THE MIDDLE EAST	108
A. AFTER THE U.S. INVASIONS OF AFGHANISTAN AND IRAQ, HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC CONCLUDED THAT THEY NEEDED TO REVOLUTIONIZE THEIR ACCESS TO U.S. TECHNOLOGIES THROUGH CORRUPT CORPORATE PARTNERS	108
B. HEZBOLLAH, THE QOD FORCE, AND REGULAR IRGC ADDRESSED THE CONSPIRACY’S FUNDING AND LOGISTICS NEEDS BY MILITARIZING THE IRANIAN TELECOMMUNICATIONS INDUSTRY AND SEIZING CONTROL OF IRAN’S LARGEST TELECOMMUNICATIONS COMPANIES IN ORDER TO ACQUIRE THE COMMUNICATIONS TECHNOLOGIES, CASH FLOW, LOGISTICAL SUPPORT, FINANCIAL MANAGEMENT SUPPORT, OPERATIONAL SUPPORT, MANAGEMENT CONSULTING SUPPORT, AND CRISIS RESPONSE SUPPORT FROM CORPORATE PARTNERS NECESSARY TO SUSTAIN A TWENTY-YEAR TERRORIST CAMPAIGN AGAINST AMERICANS	116
1. MTN Irancell	117
2. Telecommunications Company Of Iran (TCI).....	120
V. DEFENDANTS FURTHERED THE CONSPIRACY AND TRANSACTED BUSINESS WITH FRONTS, OPERATIVES, AND AGENTS CONTROLLED BY HEZBOLLAH, THE QODS FORCE AND REGULAR IRGC	121
A. THE BONYAD MOSTAZAFAN	121
B. IRAN ELECTRONICS INDUSTRIES	128
C. MTN IRANCELL	129
D. TELECOMMUNICATIONS COMPANY OF IRAN (TCI).....	130
E. THE AKBARI FRONT COMPANIES	132
F. EXIT40	133
VI. EACH DEFENDANT AND CO-CONSPIRATOR ENGAGED IN COMMERCIAL TRANSACTIONS THAT IT KNEW WERE STRUCTURED TO FINANCE, ARM, AND/OR OPERATIONALLY SUPPORT HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AND THEIR TERRORIST PROXIES IN AFGHANISTAN.....	134
A. CO-CONSPIRATOR MTN GROUP	134

1.	MTN Group Entered Its Transnational Corporate Alliance With Hezbollah, The Qods Force, And Regular IRGC In Order To Seize The “Virgin” Telecom Markets In Iran, Afghanistan, Syria, Yemen, And Lebanon, Each Of Which Was Controlled, Contested, Or Influenced By The IRGC And Its Terrorist Proxies.....	134
2.	MTN Group, MTN Dubai, And All MTN Subsidiaries And Affiliates Worldwide Joined The Terrorist Conspiracy.....	136
i.	MTN Group Effectively Serves As A Joint Venture Partner With MTN Irancell And Its Iranian Shareholders, The IRGC, Including Its Hezbollah Division And Qods Force.....	136
ii.	On September 18, 2005, MTN Group’s CEO And President Caused Every MTN Entity Worldwide To Join the Terrorist Conspiracy When He Executed The IRGC’s “Security” Agreement On Behalf Of MTN Group, MTN Dubai, And All MTN Subsidiaries, i.e., “MTN”	138
iii.	After Joining The Conspiracy, MTN Group And MTN Dubai Routinely Acted In Furtherance Of The Conspiracy	139
iv.	MTN Group’s And MTN Dubai’s Recent Conduct Demonstrates That MTN Group And MTN Dubai Remain Active Co-Conspirators With Foreign Terrorist Organizations.....	140
3.	MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC’s, Including Hezbollah’s And The Qods Force’s, Terrorist Enterprise Against Americans Worldwide	157
i.	MTN Assumed A Financial Role In The Terrorist Enterprise.....	162
a.	MTN’s Bribes to Terrorist Fronts.....	162
b.	MTN’s License Fee Payments to Terrorist Fronts	163
c.	MTN’s Funding of Terrorist Fronts through MTN Irancell Cash Flow	164
ii.	MTN Assumed An Operational Role In The Terrorist Enterprise.....	165
4.	MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban’s, Including The Haqqani Network’s, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq.....	182
5.	MTN’s Acts In Furtherance Of The Conspiracy Had A Substantial Nexus To The United States	190

i.	From 2012 Through 2019, MTN Group Regularly Reached Into The United States In Order To Unlock The U.S. Financial System So That MTN Group Could Repatriate Hundreds Of Millions Of Dollars Out Of MTN Irancell	192
ii.	MTN Group Facilitated A \$400,000 Bribe That Flowed Through The New York Financial System To A Cut-Out For The IRGC And Into The Budget Of Hezbollah, The Qods Force, And Regular IRGC	194
iii.	MTN Group And MTN Dubai Conspired To Provide, And Did Provide, A Stable, Robust, And Devastating Pipeline Of Illicitly Acquired State-of-the-Art American Technologies To Hezbollah, The Qods Force, And Regular IRGC, Including Untraceable American Smartphones.....	195
iv.	MTN Obtained U.S. Technology For The Benefit Of Hezbollah, The Qods Force, And Regular IRGC.....	197
v.	MTN Obtained Essential U.S. Services That Aided Hezbollah's, the Qods Force's, and Regular IRGC's Terrorist Capabilities	198
B.	THE ZTE DEFENDANTS	199
1.	ZTE Joined The Terrorist Conspiracy	199
i.	Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts Including But Not Limited To MTN Irancell, TCI, and Exit40, ZTE Agreed To Join A Company-Wide Conspiracy	199
ii.	ZTE, ZTE USA, And ZTE TX Each Made Overt Acts In Furtherance Of The Conspiracy	200
2.	ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Enterprise Against Americans Worldwide	200
i.	ZTE Corp., ZTE USA, And ZTE TX Knowingly Facilitated MTN Irancell And TCI's Acquisition Of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies.....	201
ii.	ZTE Corp., ZTE USA, And ZTE TX Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies.....	212

iii.	ZTE Corp., ZTE USA, And ZTE TX Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies.....	212
3.	ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq.....	215
4.	ZTE's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Including Its Haqqani Network, Comports With ZTE's Historical Sales Practices In International Markets.....	221
5.	ZTE's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Including Its Haqqani Network, Had A Substantial Nexus To The United States	224
i.	ZTE's Conduct Targeted the United States	224
ii.	ZTE's Conduct Relied on American Contacts.....	234
C.	THE HUAWEI DEFENDANTS	237
1.	Huawei Joined The Terrorist Conspiracy	237
i.	Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts, Including But Not Limited to TCI And Exit40, Huawei Agreed To Join A Company-Wide Conspiracy	237
ii.	Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Each Made Overt Acts In Furtherance Of The Conspiracy.....	238
2.	Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC's, Including its Hezbollah Division's And Qods Force's, Terrorist Enterprise Against Americans Worldwide	238
i.	Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Knowingly Facilitated MTN Irancell And TCI Acquisition of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies	239
ii.	Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed American Technology, Which Flowed Through To The IRGC's Terrorist Proxies.....	252
iii.	Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Routed Bribes To The Key Procurement Decisionmakers At	

MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies.....	253
iv. Huawei Co, Huawei USA, Huawei Device USA, Futurewei, And Skycom Routed “Free Goods” To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies	254
3. Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq	254
4. Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al- Qaeda, And The Taliban, Including Its Haqqani Network, Comports With Huawei's Historical Sales Practices In International Markets.....	261
5. Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al- Qaeda, And The Taliban, Including Its Haqqani Network, Had A Substantial Nexus To The United States	263
i. Huawei's Conduct Targeted The United States	263
ii. Huawei's Conduct Relied On American Contacts.....	267
VII. DEFENDANTS' TRANSACTIONS WITH FRONTS, OPERATIVES, AND AGENTS OF HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL- QAEDA, AND THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, CAUSED FUNDS, ARMS, LOGISTICAL AID, AND OPERATIONAL SUPPORT TO FLOW THROUGH SUCH TRANSACTIONS TO AL-QAEDA AND TALIBAN TERRORISTS ND AIDED AL-QAEDA'S AND THE TALIBAN'S ATTACKS AGAINST AMERICANS IN AFGHANISTAN	270
A. HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC SOURCED WEAPONS, RAISED FUNDS, AND OBTAINED LOGISTICAL AND OPERATIONAL SUPPORT THROUGH ILLICIT CORPORATE TRANSACTIONS IN THE TELECOM, COMMUNICATIONS, AND IT SECTORS	270
B. DEFENDANTS MADE ILLICIT DEALS WITH HEZBOLLAH, QODS FORCE, AND REGULAR IRGC FRONTS, OPERATIVES, AGENTS, AND CUT-OUTS THAT CAUSED SECURE AMERICAN SMARTPHONES, ENTERPRISE LEVEL SERVERS, NETWORK COMPUTING TECHNOLOGIES, AND WEAPONS TO FLOW THROUGH THE IRGC TO AL-QAEDA AND THE TALIBAN AND FACILITATE TERRORIST ATTACKS ON AMERICANS IN AFGHANISTAN	273

C.	DEFENDANTS MADE ILLICIT DEALS WITH HEZBOLLAH, QODS FORCE, AND REGULAR IRGC FRONTS, OPERATIVES, AGENTS, AND CUT-OUTS THAT CAUSED SUBSTANTIAL FUNDS TO FLOW THROUGH THE IRGC TO AL-QAEDA AND THE TALIBAN AND FACILITATED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN	276
1.	Procurement Bribery	277
2.	“Free Goods”	279
3.	Exit40	281
i.	Exit40 Was An IRGC Front.....	281
ii.	Co-Conspirator MTN Group Knowingly Used Exit40 To Finance Hezbollah And The Qods Force	282
iii.	ZTE Corp. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force	283
iv.	Huawei Co. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force.....	284
D.	DEFENDANTS’ PROTECTION PAYMENTS TO THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, DIRECTLY AIDED TERRORIST ATTACKS ON AMERICANS IN AFGHANISTAN	286
1.	Defendants’ Cash Protection Payments To The Taliban, Including Its Haqqani Network, Directly Funded Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan	288
2.	Defendants’ “Free Goods” Protection Payments To The Taliban, Including Its Haqqani Network, Directly Funded, Armed, And Logistically Supported Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan.....	293
VIII.	DEFENDANTS KNEW THAT THEIR TRANSACTIONS WITH HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, FACILITATED EVERY NODE OF THE CONSPIRACY AND DIRECTLY AIDED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN	298
A.	DEFENDANTS KNEW THEIR TRANSACTIONS WITH HEZBOLLAH, QODS FORCE, AND REGULAR IRGC FRONTS, OPERATIVES, AGENTS, AND CUT-OUTS FURTHERED THE IRGC’S CONSPIRACY TO ATTACK AMERICANS IN AFGHANISTAN.....	298

1.	Command, Control, Communications, And Intelligence.....	314
2.	Terrorist Finance	317
	i. Cash Flow From MTN Irancell And TCI Revenue	317
	ii. Cash Flow From Terrorist Fundraising Campaigns, Procurement Bribery, Khums, And Financial Management	322
3.	Weapons.....	323
	i. Improvised Explosive Devices (IEDs)	323
	ii. Rockets.....	324
4.	Recruiting, Fundraising, Strategic Communications, And Disinformation.....	325
	i. Recruiting and Fundraising	326
	ii. Strategic Communications and Disinformation	328
B.	DEFENDANTS KNEW THAT THEIR PROVISION OF “SECURITY” “COOPERATION” AID TO HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC SUPPORTED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN BY IRGC PROXIES AL-QAEDA AND THE TALIBAN BECAUSE DEFENDANTS KNEW THAT “SECURITY” WAS AN IRGC EUPHEMISM FOR THE IRGC PROXY ATTACKS AGAINST AMERICANS	334
1.	In-Person IRGC Communications as Terrorist Tradecraft	334
2.	Iranian Constitution	335
3.	Iranian National Security Council	335
4.	Hezbollah Structure	336
5.	IRGC Doctrine	336
6.	Iran-Focused Scholars.....	337
7.	Terrorist Statements	338
8.	Iran-Related “Security” Media Coverage	339
9.	“Security” Euphemism-Related Media Coverage	342
10.	Each Defendant’s or Co-Conspirator’s Consciousness of Guilt.....	344

C.	DEFENDANTS KNEW THEIR ILLICIT TRANSFERS OF CELL PHONES TO HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC AIDED THE CONSPIRACY’S TERRORIST ATTACKS AGAINST AMERICANS WORLDWIDE	346
D.	DEFENDANTS KNEW THAT THEIR PROTECTION PAYMENTS TO THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, FACILITATED TERRORIST ATTACKS BY AL-QAEDA AND THE TALIBAN AGAINST AMERICANS IN AFGHANISTAN AND WERE OPPOSED BY THE U.S. GOVERNMENT FOR THAT REASON.....	349
1.	Defendants Knew That Their Cash And “Free Goods” Protection Payments To The Taliban, Including Its Haqqani Network, Financed, Armed, And Logistically Sustained Terrorist Attacks By Al-Qaeda And The Taliban Against Americans In Afghanistan	349
2.	Defendants Knew That Their The U.S. Government Opposed Defendants’ Payment Of Protection Money To The Taliban, Including Its Haqqani Network.....	361
IX.	DEFENDANTS’ FINANCIAL, LOGISTICAL, AND OPERATIONAL ASSISTANCE TO THE IRGCAND PROTECTION PAYMENTS TO THE TALIBAN FLOWED THROUGH TO FACILITATE TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN THAT WERE PLANNED, AUTHORIZED, AND SOMETIMES JOINTLY COMMITTED BY AL-QAEDA	369
A.	IN FURTHERANCE OF THE IRGC CONSPIRACY, THE IRGC RELIED UPON DEFENDANTS’ RESOURCES TO PROVIDE KEY ASSISTANCE TO AL-QAEDA AND THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, THAT FACILITATED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN IN ORDER TO DRIVE THE UNITED STATES OUT OF AFGHANISTAN IN FURTHERANCE OF THE IRGC’S CONSPIRACY	369
1.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support For Anti-American Terrorism In Afghanistan To Undermine The U.S. Mission There	370
2.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban, Including its Haqqani Network, With Weapons, Explosives, And Lethal Substances.....	379
3.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Lodging, Training, Expert Advice Or Assistance, Safehouses, Personnel, And Transportation	383
4.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Financial Support.....	387

5.	The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support to Al-Qaeda to Facilitate Syndicate Attacks in Afghanistan	389
B.	IN FURTHERANCE OF THE IRGC CONSPIRACY, AL-QAEDA AUTHORIZED AND PLANNED THE ATTACKS THAT INJURED PLAINTIFFS	396
1.	Al-Qaeda Authorized the Attacks that Injured Plaintiffs.....	396
2.	Al-Qaeda Planned the Attacks that Injured Plaintiffs.....	398
i.	Al-Qaeda Planned the IED Attacks that Injured Plaintiffs	401
ii.	Al-Qaeda Planned the Suicide Attacks that Injured Plaintiffs.....	407
C.	IN FURTHERANCE OF THE IRGC CONSPIRACY, AL-QAEDA COMMITTED TERRORIST ATTACKS THAT KILLED AND INJURED PLAINTIFFS IN JOINT CELLS WITH THE TALIBAN, LASHKAR-E-TAIBA, AND JAISH-E-MOHAMMED	409
1.	The “N2KL” Provinces: Al-Qaeda Committed the Attacks in Nangarhar, Nuristan, Kunar and Laghman that Injured Plaintiffs.....	410
2.	The “P2K” Provinces: Al-Qaeda Committed the Attacks in Paktia, Paktika, and Khost that Injured Plaintiffs	411
3.	Kabul Attack Network-Related Provinces: Al-Qaeda Committed the Kabul Attack Network Attacks that Injured Plaintiffs.....	412
X.	THE IRGC-BACKED TALIBAN TERRORIST SYNDICATE IN AFGHANISTAN AND PAKISTAN LED BY AL-QAEDA AND THE TALIBAN KILLED AND INJURED THE PLAINTIFFS WHO WERE ATTACKED IN AFGHANISTAN IN 2012 THROUGH 2018 THROUGH TERRORIST ATTACKS FOR WHICH DEFENDANTS PROVIDED SUBSTANTIAL ASSISTANCE	413
A.	APRIL 4, 2012 ATTACK IN FARYAB (FAMILIES OF DAVID W. LAU, CHRISTOPHER J. ROSEBROCK, AND NICHOLAS ROZANSKI)	414
1.	The David Lau Family	415
2.	The Nicholas Rozanski Family	416
3.	Christopher Rosebrock.....	416
B.	APRIL 22, 2012 ATTACK IN GHAZNI (MICHAEL METCALF FAMILY)	417

C.	MAY 6, 2012 ATTACK IN PAKTIA (FAMILIES OF THOMAS FOGARTY AND JONATHAN CLEARY)	418
1.	The Thomas Fogarty Family	418
2.	The Jonathan Cleary Family	419
D.	MAY 7, 2012 ATTACK IN GHAZNI (FAMILIES OF CHASE MARTA AND JACOB SCHWALLIE)	420
1.	The Chase Marta Family	420
2.	The Jacob Schwallie Family	421
E.	MAY 13, 2012 ATTACK IN KHOST (RICHARD MCNULTY III FAMILY)	421
F.	MAY 18, 2012 ATTACK IN KUNAR (MICHAEL KNAPP FAMILY)	423
G.	MAY 20, 2012 ATTACK IN KANDAHAR (ERIC LUND FAMILY)	423
H.	MAY 20, 2012 ATTACK IN URUZGAN (RYAN TIMONEY FAMILY)	424
I.	MAY 23, 2012 ATTACK IN KANDAHAR (TRAVIS MORGADO FAMILY)	425
J.	MAY 30, 2012 ATTACK IN KANDAHAR (NICHOLAS OLIVAS FAMILY)	427
K.	MAY 31, 2012 ATTACK IN HELMAND (ERIC HUNTER FAMILY)	428
L.	JUNE 12, 2012 ATTACK IN HELMAND (ERICH ELLIS FAMILY)	429
M.	JANUARY 12, 2012 ATTACK IN KANDAHAR (TREVOR PINNICK FAMILY)	430
N.	JULY 8, 2012 ATTACK IN WARDAK (FAMILIES OF CAMERON STAMBAUGH AND CLARENCE WILLIAMS III)	431
1.	The Cameron Stambaugh Family	431
2.	The Clarence Williams III Family	432
O.	JULY 13, 2012 ATTACK IN ZABUL (MICHAEL RISTAU FAMILY)	433
P.	JULY 19, 2012 ATTACK IN HELMAND (JOSHUA ASHLEY FAMILY)	434
Q.	JULY 22, 2012 ATTACK IN LOGAR (JUSTIN HORSLEY FAMILY)	435
R.	JULY 22, 2012 IN HERAT (JOSEPH PEREZ FAMILY)	436

S.	AUGUST 1, 2012 ATTACK IN PAKTIKA (TODD LAMBKA FAMILY).....	437
T.	AUGUST 7, 2012 ATTACK IN PAKTIA (ETHAN MARTIN FAMILY).....	438
U.	AUGUST 8, 2012 ATTACK IN KUNAR (KEVIN GRIFFIN FAMILY).....	439
V.	AUGUST 16, 2012 ATTACK IN KANDAHAR (RICHARD ESSEX FAMILY).....	441
W.	SEPTEMBER 1, 2012 ATTACK IN GHAZNI (FAMILIES OF JEREMIE S. BORDER AND JONATHAN SCHMIDT).....	441
1.	The Jeremie S. Border Family	442
2.	The Jonathan P. Schmidt Family	442
X.	SEPTEMBER 13, 2012 ATTACK IN GHAZNI (KYLE OSBORN FAMILY).....	443
Y.	SEPTEMBER 15, 2012 ATTACK IN HELMAND (FAMILIES OF BRADLEY W. ATWELL AND CHRISTOPHER K. RAIBLE).....	444
1.	The Bradley W. Atwell Family.....	445
2.	The Christopher K. Raible Family.....	445
Z.	SEPTEMBER 16, 2012 ATTACK IN ZABUL (JON TOWNSEND FAMILY).....	446
AA.	SEPTEMBER 17, 2012 ATTACK IN KANDAHAR (KEVIN TRIMBLE)	446
BB.	SEPTEMBER 26, 2012 ATTACK IN LOGAR (FAMILIES OF JONATHAN GOLLNITZ AND ORION SPARKS).....	447
1.	The Jonathan Gollnitz Family.....	448
2.	The Orion Sparks Family.....	449
CC.	OCTOBER 1, 2012 ATTACK IN KHOST (JEREMY HARDISON FAMILY).....	450
DD.	OCTOBER 22, 2012 ATTACK IN KANDAHAR (EDWARD KLEIN)	451
EE.	NOVEMBER 3, 2012 ATTACK IN PAKTIKA (RYAN P. JAYNE FAMILY).....	452
FF.	NOVEMBER 16, 2012 ATTACK IN PAKTIKA (JOSEPH A. RICHARDSON FAMILY).....	453
GG.	NOVEMBER 18, 2012 ATTACK IN HELMAND (DALE MEANS FAMILY).....	455

HH.	DECEMBER 15, 2012 ATTACK IN KABUL (MARK SCHOONHOVEN FAMILY).....	456
II.	FEBRUARY 22, 2013 ATTACK IN HELMAND (JONATHAN D. DAVIS FAMILY).....	458
JJ.	MARCH 11, 2013 ATTACK IN WARDAK (REX L. SCHAD FAMILY)	459
KK.	APRIL 6, 2013 ATTACK IN ZABUL (ANNE T. SMEDINGHOFF FAMILY).....	459
LL.	MAY 4, 2013 ATTACK IN KANDAHAR (FAMILIES OF KEVIN CARDOZA, BRANDON J. LANDRUM, THOMAS P. MURACH, FRANCIS G. PHILLIPS IV, AND BRANDON J. PRESCOTT)	461
1.	The Kevin Cardoza Family	462
2.	The Brandon J. Landrum Family	462
3.	The Thomas P. Murach Family	463
4.	The Francis G. Phillips IV Family	464
5.	The Brandon J. Prescott Family	464
MM.	MAY 14, 2013 ATTACK IN KANDAHAR (FAMILIES OF MITCHELL DAEHLING AND WILLIAM J. GILBERT).....	465
1.	The Mitchell Daehling Family	466
2.	The William J. Gilbert Family	466
NN.	MAY 16, 2013 ATTACK IN KABUL (ANGEL ROLDAN JR. FAMILY).....	467
OO.	JUNE 2, 2013 ATTACK IN HELMAND (SEAN W. MULLEN FAMILY)	469
PP.	JUNE 18, 2013 ATTACK IN PARWAN (ROBERT W. ELLIS FAMILY).....	470
QQ.	JUNE 23, 2013 ATTACK IN PAKTIKA (BRANDON KORONA)	471
RR.	JULY 15, 2013 ATTACK IN PAKTIKA (SONNY C. ZIMMERMAN FAMILY).....	472
SS.	JULY 23, 2013 ATTACK IN WARDAK (FAMILIES OF ROB L. NICHOLS AND NICKOLAS S. WELCH).....	473
1.	The Rob L. Nichols Family	473
2.	The Nickolas S. Welch Family	474

TT.	JULY 30, 2013 ATTACK IN LOGAR (NICHOLAS B. BURLEY FAMILY).....	475
UU.	AUGUST 12, 2013 ATTACK IN LOGAR (JAMES T. WICKLIFF CHACIN FAMILY).....	476
VV.	SEPTEMBER 21, 2013 ATTACK IN PAKTIA (FAMILIES OF LIAM NEVINS AND JOSHUA J. STRICKLAND).....	477
1.	The Liam Nevins Family	478
2.	The Joshua J. Strickland Family	478
WW.	SEPTEMBER 26, 2013 ATTACK IN PAKTIA (THOMAS A. BAYSORE JR. FAMILY).....	479
XX.	OCTOBER 6, 2013 ATTACK IN KANDAHAR (FAMILIES OF CODY PATTERSON AND JOSEPH M. PETERS)	480
1.	The Cody Patterson Family	480
2.	The Joseph M. Peters Family.....	481
YY.	FEBRUARY 10, 2014 ATTACK IN KABUL (FAMILIES OF PAUL GOINS JR. AND MICHAEL A. HUGHES).....	482
1.	The Paul Goins Jr. Family	483
2.	The Michael A. Hughes Family.....	484
ZZ.	FEBRUARY 15, 2014 ATTACK IN HELMAND (AARON C. TORIAN FAMILY).....	484
AAA.	AUGUST 12, 2014 ATTACK IN KANDAHAR (ALBERTO DIAZ FAMILY).....	485
BBB.	NOVEMBER 24, 2014 ATTACK IN KABUL (JOSEPH RILEY FAMILY).....	487
CCC.	DECEMBER 12, 2014 ATTACK IN PARWAN (WYATT J. MARTIN FAMILY).....	489
DDD.	JANUARY 29, 2015 ATTACK IN KABUL (JASON D. LANDPHAIR FAMILY).....	490
EEE.	AUGUST 22, 2015 ATTACK IN KABUL (FAMILIES OF COREY J. DODGE, RICHARD P. MCEVOY, AND BARRY SUTTON)	491
1.	The Corey J. Dodge Family	492
2.	The Richard P. McEvoy Family	493

3.	The Barry Sutton Family	494
FFF.	AUGUST 26, 2015 ATTACK IN HELMAND (MATTHEW D. ROLAND FAMILY).....	494
GGG.	DECEMBER 21, 2015 ATTACK IN PARWAN (CHESTER J. MCBRIDE III FAMILY).....	495
HHH.	JANUARY 5, 2016 ATTACK IN HELMAND (MATTHEW Q. MCCLINTOCK FAMILY)	497
III.	AUGUST 7, 2016 ATTACK IN KABUL (KEVIN KING FAMILY).....	498
JJJ.	THE JUNE 10, 2017 ATTACK IN NANGARHAR (FAMILIES OF WILLIAM M. BAYS AND DILLON C. BALDRIDGE).....	499
1.	The William M. Bays Family	500
2.	The Dillon C. Baldrige Family	501
KKK.	JULY 3, 2017 FIRE ATTACK IN HELMAND (HANSEN B. KIRKPATRICK FAMILY).....	501
COUNT ONE	503
COUNT TWO	506
COUNT THREE	511

INTRODUCTION

1. This lawsuit seeks damages under the federal Anti-Terrorism Act (the “ATA”) on behalf of American service members and civilians, and their families, who were killed or wounded while serving their country in Afghanistan between 2012 and 2017. Plaintiffs seek to hold ZTE and Huawei, two Chinese telecom companies and technology manufacturers, accountable for their conspiracy with, and substantial assistance to, multiple Foreign Terrorist Organizations (“FTOs”) targeting Americans in Iraq, Afghanistan, the Middle East, and Europe.

2. A third company, MTN, a South African technology company that focused on telecoms, was also a key participant in the conspiracy alleged herein. While not a co-defendant in this case, MTN’s conduct demonstrates what ZTE and Huawei also did because ZTE and Huawei (alongside co-conspirator MTN) all responded to the same requests for assistance from the same terrorist groups in the same markets at the same time.

3. Plaintiffs’ allegations are based on information derived from confidential witnesses with direct and indirect knowledge of the alleged facts, internal company documents, declassified military-intelligence reporting, congressional testimony and reports, press accounts, and Plaintiffs’ recollections.

4. ZTE and Huawei (alongside co-conspirator MTN) are large multinational companies that had lucrative business in Iran and Afghanistan that relied upon regular transactions with counterparties that ZTE and Huawei (alongside co-conspirator MTN) knew served as fronts for terrorist finance and logistics, and ZTE and Huawei (alongside co-conspirator MTN) engaged in illicit, terrorism-sanctions-busting transactions with known terrorist fronts in order to boost their profits. Those transactions aided and abetted terrorism by directly funding, arming, and logistically supporting a terrorist campaign in Afghanistan that stretched for nearly two decades, killing and injuring thousands of Americans.

5. ZTE and Huawei (alongside co-conspirator MTN) provided two separate streams of devastating assistance that ultimately flowed to benefit the al-Qaeda and Taliban terrorists in Afghanistan who killed and injured Plaintiffs or their family members in attacks from 2012 through 2017.

6. *First*, ZTE and Huawei (alongside co-conspirator MTN) directly provided funding, technology, weapons, services, and other assistance to the world's worst sponsor of terrorism, Iran's Islamic Revolutionary Guards Corps (or "IRGC"), including its Lebanese Hezbollah Division and Qods Force, in furtherance of the IRGC's conspiracy to target and kill Americans in the Middle East, including Afghanistan, in order to drive the United States from the region. The IRGC relied upon such aid to facilitate attacks by its proxies in Afghanistan, al-Qaeda and Iraq, both of whom joined the IRGC's conspiracy to expel the United States from the countries on Iran's borders, Afghanistan and Iraq. Such assistance flowed through the IRGC, including through Hezbollah and the Qods Force, and reached al-Qaeda and the Taliban, who deployed the IRGC's aid to sustain a successful nearly two-decades-long terrorist campaign against Americans there.

7. *Second*, ZTE and Huawei (alongside co-conspirator MTN) made substantial protection payments, in cash and "free goods," to the Taliban, including its Haqqani Network, in order to further the IRGC's conspiracy and also redirect violence away from ZTE's and Huawei's (alongside co-conspirator MTN's) shipments, facilities, and projects in Afghanistan. ZTE's and Huawei's (alongside co-conspirator MTN's) protection payments to the Taliban provided an equally potent stream of assistance to the terrorists, directly funding, arming, and logistically sustaining the Taliban, including its Haqqani Network.

8. This case reveals conduct that is far more depraved than even the ordinarily culpable ATA defendant. Few ATA defendants have ever been credibly accused of the full spectrum of behavior identified in this Complaint against ZTE and Huawei, both of whom directly conspired with known fronts for designated terrorist organizations. In serving as full-spectrum telecommunications and computing partners for Hezbollah, the Qods Force, and Regular IRGC and, through these IRGC components, for long-standing IRGC proxies like al-Qaeda and the Taliban, ZTE and Huawei aided *every* facet of the IRGC's terrorist enterprise and the broader IRGC Conspiracy that it served. Moreover, by making protection payments to the Taliban, including its Haqqani Network, ZTE and Huawei provided a second equally potent stream of value that also provided cross-cutting financial, logistical, and operational benefits to the terrorists who committed the attacks that injured Plaintiffs and their loved ones.

9. ZTE and Huawei (alongside co-conspirator MTN) aided the terrorists because they were co-conspirators with the IRGC, as each signed written agreements pledging to support the "security" agenda of their counterparty "Iranian Shareholders" – which were themselves fronts for the IRGC – which they and the IRGC both knew meant supporting the IRGC's, including Hezbollah's and the Qods Force's, industrial-scale exportation of terror targeting Americans around the world, but most of all, in the two countries flanking Iran: Iraq to the west, and Afghanistan to the east.

10. Here's how the conspiracy worked. The IRGC led a conspiracy, the object of which was to commit terrorist attacks on Americans in the countries bordering Iran, Afghanistan and Iraq (the "IRGC Conspiracy").

11. The IRGC established the IRGC Conspiracy after 9/11 and it continued until the end of the conflict in Afghanistan.

12. The co-conspirators along with the IRGC in the IRGC Conspiracy included the terrorist organizations integral to or supported by the IRGC, including its subordinate Hezbollah Division and Qods Force, al-Qaeda, the Taliban, including its Haqqani Network, and others. Corporate fronts for the IRGC, including the telecom companies the IRGC controlled such as MTN Irancell, the Telecommunications Company of Iran (“TCI”), and Mobile Communication Co of Iran (“MCI”) were also co-conspirators.

13. The IRGC Conspiracy operated through its terrorist members to carry out attacks on Americans, with the IRGC providing logistical and financial support. The attacks in this case were all acts in furtherance of the IRGC Conspiracy. Every person and entity that agreed to join the IRGC Conspiracy is therefore liable for the harm caused by these attacks.

14. ZTE and Huawei (alongside co-conspirator MTN) joined the IRGC Conspiracy on the specific dates they agreed with known IRGC fronts (variously, MTN Irancell, TCI, and MCI) to provide resources, technical materials, and technical support, and to support Iran’s “security” objectives.

15. Each of ZTE and Huawei (alongside co-conspirator MTN) acted in furtherance of that agreement to join the IRGC Conspiracy each time they provided money and other resources, provided technical goods, such as cell phones and telecom infrastructure, assisted with technical support, as was their obligation as joint venturers with and contractual counterparties to known IRGC fronts, when they evaded U.S. sanctions in order to do so, and when they attempted to obfuscate their respective roles. Each time ZTE and Huawei (alongside co-conspirator MTN) did these acts in furtherance of the IRGC Conspiracy, such person assisted the IRGC Conspiracy’s objective to attack Americans and furthered the IRGC Conspiracy’s ultimate objective to expel the U.S. from Afghanistan and Iraq.

16. ZTE and Huawei (alongside co-conspirator MTN), entered into the IRGC Conspiracy with the IRGC, and acted in furtherance thereof in programmatic, and enduring ways for well over a decade. ZTE and Huawei (alongside co-conspirator MTN) were one in spirit with their IRGC terrorist partners because each calculated that, if they remained aligned with the interests of their partners' "Iranian Shareholders" – fronts for the IRGC – their company would reap billions in profits by seizing a monopoly in one of the world's fastest-growing and youngest potential subscriber pools.

17. To earn their billions, ZTE and Huawei (alongside co-conspirator MTN) simply needed to believe that the obvious, and vast, American bloodshed in Afghanistan and Iraq that was sure to follow their decision was an acceptable price to pay to yield a profitable outcome for their own shareholders and the "Iranian Shareholders" with whom they were at times joint venture partners and at others explicit contractual counterparties.

18. Seasoned investors, however, know that any time one shareholder's investment does well, that means somewhere out there is another shareholder on the opposite side of the issue, for whom the investment went badly.

19. For every shareholder who wins, there must be another shareholder in the world who loses. But this is not a case about trading shares on the NASDAQ. In this case, the "shareholders" who lost were not day traders who got crushed making an unwise stock pick. They were the Plaintiffs, and others.

20. Plaintiffs were patriotic American servicemembers and civilians who volunteered for hard, thankless, jobs on the other side of the world in Afghanistan. Some returned, badly injured. Some never came back at all. None will ever be the same again. ZTE and Huawei

(alongside co-conspirator MTN) played an enormous role in the sequence of events that led to this outcome. Plaintiffs are among the victims. This lawsuit followed.

21. It is impossible to overstate the magnitude of ZTE's and Huawei's defilement of the Anti-Terrorism Act. This case concerns one of the single most depraved, expansive, deceitful, and persistent international corporate conspiracies since the end of World War II, led by the IRGC and enabled by their corporate co-conspirators, ZTE and Huawei (alongside co-conspirator MTN). There is little doubt that the IRGC conspiracy changed the trajectory of Afghanistan, Iraq, and countless other countries.

22. This Complaint outlines the unprecedented nature of ZTE's and Huawei's conduct, and it likely remains the tip of the iceberg. Few other defendants in the history of the ATA have engaged in conduct as comprehensively violative, for more money, over a longer period, with a more violent counterparty, with more devastating consequences, while demonstrating a greater sense of corporate impunity. For more than a decade, ZTE and Huawei funded, partnered with, and helped develop the technical capabilities for the world's worst terrorist organization – the IRGC – by entering into deals with notorious fronts for the IRGC and pledging to assist with Iran's "security" agenda – all while fraudulently concealing it from everyone, including their own shareholders. While doing so, ZTE and Huawei – like their co-conspirator MTN – also made protection payments directly to the IRGC's Afghanistan proxies, the Taliban, including its Haqqani Network.

23. ZTE and Huawei are two of the worst corporate sponsors of terrorism in the history of the ATA. And because their behavior mirrored that of a co-conspirator, MTN, this case is likely to be different than a typical ATA case because of what ZTE and Huawei have done, and this Complaint is longer than many ATA complaints. ZTE and Huawei each funneled

hundreds of millions in value to the terrorists in nearly every conceivable modality of terrorist fund transfer: direct transactions with FTO fronts while knowing (and not caring) about the FTO relationship; illicit acquisition of valuable American technologies; procurement bribes; “free goods” kickbacks; black market purchasing; cash flow from the companies; and so on.

24. The evidence regarding these co-conspirators’ intent is even worse. Like the IRGC fronts with whom they did business, ZTE and Huawei made shocking admissions in writing, and then destroyed everything to try to cover their tracks (none succeeded completely). Some Defendants lied to federal law enforcement. Witness intimidation was common. Innocent Canadians were kidnapped to extort the United States and Canada.

25. ZTE’s and Huawei’s conduct, spending amount, and terrorist tradecraft is startlingly like how a State Sponsor of Terrorism acts—hundreds of millions of dollars in direct funding to terrorists, critical technical support that aids their victory given with the hope that it will occur, and a commitment to never-ending lies, falsehoods, and deceptions no matter how much evidence accumulates or how ridiculous it becomes.

26. ZTE and Huawei may have learned this “never stop lying” tactic at the feet of their client, the IRGC, which is notorious amongst national security professionals for, in effect, being some of the world’s most persistent long-term liars, capable of sustaining a lie for decades. ZTE and Huawei made similar choices.

27. To make billions of dollars running the phone system and internet working with these people in partnership, ZTE and Huawei (alongside their co-conspirator MTN) had to fully commit themselves worldwide to corporate criminality on an almost impossible to comprehend scale. These three companies combined to enable unprecedented aid to terrorists, which included, among other things:

- a secret, undisclosed, direct, written, terrorist joint venture agreement signed by an active, senior-ranks Iranian terrorist, on the one hand, and the CEO of one of Africa's largest publicly traded companies (MTN), on the other;
- direct contractual obligations with Iranian entities known to be owned and controlled by fronts for the IRGC, whereby substantial banned technology useful to terrorists was transferred, and entire telecommunication systems used by the terrorist conspirators were assembled, used, and maintained;
- a nearly two decade-long conspiracy that operationalized the secret deal into a technological, financial, services, and communications supply chain for the world's worst transnational terrorist organization; and
- shocking bribery, including tens of millions of "free goods" bribes designed to be diverted by terrorist to the black market, and large U.S. Dollar wire transfers after the bribe recipient performed his or her illicit deed.

28. To attack the citizens protected by the world's most powerful military in Iraq and Afghanistan and Iraq after 2003, Hezbollah, the Qods Force, and Regular IRGC organized a transnational terrorist alliance – a NATO for Islamists – that included both Shiite and Sunni, and stretched throughout the Middle East, from Syria to Afghanistan.

29. In Iraq, the IRGC helped stand up an alliance of Shiite terrorists that attacked Americans there, which was led by the IRGC's Hezbollah Division and Hezbollah's Iraqi proxy, Jaysh al-Mahdi, funded and armed by the IRGC, through Hezbollah, and operated through the IRGC's classic "joint cell" approach that emphasized close cooperation between Hezbollah, the Qods Force, and the IRGC's local terrorist proxy, Jaysh al-Mahdi. Simultaneously, the IRGC also sponsored al-Qaeda's terrorist proxies in Iraq, who shared the same goal as its Shiite proxies: kill Americans to drive the U.S. out.

30. The IRGC's ambitions did not stop at Iraq. As Hezbollah intensified its terror campaign in Iraq, the IRGC pursued a similar campaign against the Americans on Iran's other flank: Afghanistan. Like its role in Iraq, the IRGC provided comprehensive and critical support

to the leaders of the anti-American alliance in Afghanistan and Pakistan, which operated as a terrorist “Syndicate” that was led by al-Qaeda and the Taliban, including its Haqqani Network.

31. In Afghanistan, the IRGC furthered the conspiracy by funding, arming, training, logistically sustaining, and providing safe havens to al-Qaeda and the Taliban, including its Haqqani Network, who followed a similar Joint Cells approach as the IRGC, and for similar reasons. In the twenty years between 9/11 and the American withdrawal from Afghanistan, the IRGC, including its Hezbollah Division and Qods Force, prosecuted a grinding, global terrorist campaign, which it supported from a latticework of cells arrayed across six continents. The grim result: more than 4,000 Americans were killed in terrorist attacks in Afghanistan and Iraq by designated terrorist groups that were funded, armed, and logistically sustained by the IRGC. Indeed, each of the designated terrorist groups were members of the same global terrorist conspiracy led by the IRGC.

32. Every Plaintiff in this case is an American who was injured, or whose loved one was killed or injured, in Afghanistan between 2012 and 2017 in attacks that occurred in Afghanistan in furtherance of the IRGC Conspiracy.

33. While Plaintiffs, or their loved ones, worked to stabilize Afghanistan, they were attacked by U.S. Government-designated terrorist organizations that participated in an IRGC-backed, Hezbollah-led terrorist conspiracy campaign that ZTE’s and Huawei’s (alongside co-conspirator MTN’s) transactions helped finance, arm, logistically support, conceal, and upgrade.

34. ZTE and Huawei (alongside co-conspirator MTN) helped revolutionize the efficiency of the Big Data management practices and capabilities of Hezbollah and the Qods Force, in addition to the “regular” IRGC inside of Iran. It is impossible to overstate the scale of

the carnage that followed Defendants' decision to midwife the IRGC, including its Hezbollah Division and Qods Force, into the modern, networked, Big Data world.

35. Prior to Defendants, Hezbollah, the Qods Force, and Regular IRGC had the will but not the modern gear. While Hezbollah, the Qods Force, and Regular IRGC had the scale of a global multinational corporate behemoth – tens of thousands of personnel, consultants, agents, and partners, distributed across dozens of countries on six continents – the IRGC lacked even rudimentary network computing technologies.

36. By 2004, the IRGC was surrounded on both flanks by “the Great Satan,” and the enormous technological gap between the IRGC and its mortal enemy – the “Big Data Gap” – forced the IRGC to do something drastic, which it had never done before: bring in foreign companies to revolutionize Iran's computing and telecommunications infrastructure.

37. Two problems, however, still confronted Hezbollah, the Qods Force, and Regular IRGC. *First*, the IRGC knew that most large technology companies would have nothing at all to do with them. The IRGC also knew what any intelligence operative knows: that large telecom and networking computing companies come from a generally ethical industry that has never experienced a major terrorist finance scandal and are internationally notorious within the telecoms industry for being unabashed patriots.

38. *Second*, and worse still, if the IRGC wanted to acquire the key technologies that it had determined were essential to prosecuting its terror campaign, it could not avoid an outcome in which the IRGC, indirectly, needed to reach into America's markets, and acquire embargoed

dual-use technologies on an industrial scale while surmounting at least three separate detection hurdles,¹ in a race where any stumble would likely result in the exposure of the entire scheme.

39. The solution to both? Find some corporate criminals, bring them all the way into the circle of trust, and count on their limitless greed. Enter, Defendants. Since the 1979 revolution, the IRGC has always sought to kill Americans in large numbers. What it lacked was not the will, but the capabilities. After 9/11, the story remained the same – until ZTE and Huawei (alongside co-conspirator MTN) answered the IRGC’s call for multinational corporate assistance to the “security” operations of Hezbollah Division and the Qods Force.

40. What Hezbollah, the Qods Force, and Regular IRGC had never had – until Defendants – were true, established multinational corporate criminal partners. And Defendants furnished the IRGC two: ZTE Corporation, and Huawei Co. One has pleaded guilty (ZTE) and one is currently defending itself in a criminal trial in this District (Huawei); meanwhile, their co-conspirator is defending itself in South Africa (MTN).

41. After 9/11, the IRGC coordinated a grand alliance of Islamist terrorists to attack Americans in the Middle East. On the eve of the U.S. invasion of Iraq, the IRGC’s leadership and Hezbollah agreed to prepare, instigate, and sustain a nationwide campaign of terror against Americans in Iraq, which was planned and authorized by the IRGC’s lead foreign terror agent,

¹ Possible avenues of detection for which Hezbollah, the Qods Force, and Regular IRGC had to prepare included, but were not limited to: (1) direct or indirect communications with their operatives, agents, fronts, or cut-outs inside the United States to identify the specific U.S. technologies sought by the IRGC; (2) the illicit acquisition of such technologies inside the U.S. as requested by the IRGC; (3) the illicit export of such technologies from the U.S. to the purchasing entity outside the U.S. controlled by, or acting for the benefit for, the IRGC; and (4) the follow-on servicing of such American technologies, which ordinarily required the IRGC, through the same channels, re-engage with the U.S. persons, operating from inside the United States, whom the IRGC needed to maintain the American technology it illicitly purloined through the above avenues.

Hezbollah. To sustain an ever-escalating terrorist campaign against the United States in Iraq, and later Afghanistan, Iran relied upon Hezbollah, which, in turn, depended upon IRGC funding and illicitly sourced gear from a constellation of IRGC, including Hezbollah and the Qods Force, terrorist fundraising and logistics cells scattered across dozens of countries on six continents.

42. To sustain their insurgency, the terrorists relied upon three substantial funding streams: sources from within Iraq, most of all, the river of cash and free goods that Jaysh al-Mahdi obtained from corrupt companies doing business before the Iraqi Ministry of Health, sources from within Iran, and sources from the latticework of IRGC, Hezbollah and the Qods Force, logistics and fundraising cells that stretch the globe from Dubai to South Africa, Houston to Syria, and countless other geographies.

43. This case is about those second and third sources of funding; while the Iraqi Ministry of Health was the largest overall single source of funding for the terrorists, the second and third streams were equally potent. Cash flow from the telecom company Irancell was either the largest or second largest source of cash flow from any IRGC front and caused hundreds of millions per year to flow to the IRGC, including \$4.2 billion between 2005, when MTN Group bribed its way to the lucrative Irancell license that was controlled by the IRGC (resulting in MTN Irancell), and 2013 – approximately \$500 million per year, every year. Similarly, the global fundraising and logistics cells coordinated cash flows from narcotics smuggling, and the Qods Force’s and Hezbollah’s various transnational criminal rackets, e.g., collecting 10%-20% “taxes” as *khums* from allied businesspeople in Dubai, U.A.E., or Pretoria, South Africa.²

² *Khums* are a form of fundraising in the Islamic faith analogous to tithing in the Christian faith, under which pious Muslims contribute between 10% to 20% of their income to a designated recipient. Hezbollah, the Qods Force, and Regular IRGC al-Qaeda, and the Taliban, including its Haqqani Network, have long solicited financial contributions styled as *khums*.

44. Given the transnational nature of the conspiracy they led, the Qods Force and Hezbollah depended upon illicitly sourced, embargoed American communications and information technologies, which they acquired through ZTE Corp., ZTE TX, ZTE USA, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom (alongside their co-conspirator MTN). Defendants' conduct changed the trajectory of the entire terrorist campaign in Iraq and Afghanistan by revolutionizing the communications capabilities of both Hezbollah and the Qods Force in Iraq and throughout the Middle East and by crippling the ability of U.S. forces in Iraq to detain Qods Force and Hezbollah operatives in the region – because we could almost never find them. Because of Defendants' conspiracy, Plaintiffs suffered the consequences.

45. ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN) entered the conspiracy through secret deals to which their senior leaders agreed on their behalf, with IRGC operatives similarly agreeing on the IRGC's behalf, necessarily including the IRGC's external terrorist arms, the Qods Force and Hezbollah Divisions.

46. This case is about that IRGC structure: from the terrorists' fundraising and logistics fronts (like the terrorist front disguised as a charitable trust, the Bonyads Mostazafan) to the various strategies for illicitly sourcing U.S. Dollars and weapons technologies (like using agents, cut-outs, and intentional overpayments in Dubai), and raising money (such as through bribes, taxes, and front company cash flows), to the terrorists' strategy for concealing the scheme (through removing U.N. sanctions that interfered with front companies necessary to the scheme), to the terrorists' ability to securely communicate with one another (through illicitly obtained American phones), to the terrorists' ability to better surveil kidnapping targets and anticipatory Quick Reaction Forces in response (from enhanced computing technologies) and finally, to their ability to build more powerful and accurate roadside bombs and rockets necessary to punch

through the cocoon of armor that protected Americans (through a host of illicit technologies illegally sourced from the U.S.).

47. ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN Group and its affiliates) signed either literal terrorism joint venture agreements and/or entered into contracts with known IRGC fronts. MTN Group kept its agreement locked in a safe, concealed from the world. On information and belief, ZTE Corp. and Huawei Co., practicing better terrorist tradecraft than their sloppy co-conspirators at MTN Group, smartly destroyed their copies, but their parallel performance to MTN Group confirms their agreement all the same.

48. Ever since, publicly, ZTE and Huawei (alongside co-conspirator MTN) variously lied, dissembled, intimidated witnesses, destroyed evidence, all to avoid admitting the obvious: that they directly armed, funded, and enabled the communications of Hezbollah, the Qods Force, Regular IRGC, and the IRGC's proxies in Iraq, Iran, Lebanon, and Syria, as well as Qods Force and Hezbollah support cells from around the world, stretching from Syria to Afghanistan.

49. ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN) are each culpable. Each did, essentially, the same thing. The only difference is that MTN Group's secret vault of smoking documents were leaked by a whistleblower in March 2012, revealing the scheme MTN Group had fraudulently concealed from the world, its own shareholders, the South African government, the U.S. government, and the U.A.E. government, to name but a few.

50. The MTN Group document revelation in 2012 did not just reveal MTN Group's scheme. Critically, it outed the *IRGC's terrorist tradecraft* when it comes to virtually every facet of the terrorist logistics, funding, and communications chains. MTN Group's conduct is not just probative of what MTN Group itself did; as informed by information that emerged years later, it shows what the IRGC demanded of *every* corporate business partner in this space.

Consequently, MTN Group's conduct offers a reasonable inference regarding the conduct of ZTE Corp. and Huawei Co., as well as that of their mutual business partner – the IRGC.

51. Like MTN Group, ZTE Corp. and Huawei Co. also joined the conspiracy and also fraudulently concealed their participation by following the same Hezbollah/Qods Force playbook that MTN Group followed. Unlike MTN, however, ZTE and Huawei did not experience their own whistleblower revolts until later, but, eventually, everyone got caught. MTN Group has been enmeshed in litigation for nearly a decade. And ZTE and Huawei were both investigated by the U.S. law enforcement, with serious criminal charges flowing out of each inquiry. From these cases, there is overwhelming evidence that Hezbollah, the Qods Force, and Regular IRGC relied upon ZTE and Huawei, just as these IRGC constituents did with respect to MTN, to surreptitiously acquire U.S. Dollars and vital U.S. technologies critical to every aspect of the terrorist enterprise.

52. ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN) were one in spirit with the terrorists. Each pledged, in writing, their commitment to aiding the IRGC's "security" – which all involved understood to be a euphemism for anti-American terror. They did this because IRGC domination of the Middle East was great for each Defendants' profits and, with respect to ZTE Corp. and Huawei Co., the victory of the IRGC over the United States, served the hostile national security objectives of the Chinese Communist Party, which sought to aid Shiite terrorists in the region to inflict pain on Americans in Iraq in order to cause the United States to withdraw from the country.

53. After entering the conspiracy with known IRGC fronts called Irancell and TCI, MTN Group, ZTE Corp., Huawei Co., and their respective subsidiaries, knowingly partnered with notorious fronts for Hezbollah, such as the Bonyad Mostazafan. Through such business

ZTE and Huawei (alongside co-conspirator MTN) provided direct financial support, revenue, U.S.-origin, embargoed technology and equipment, and training and expertise—all of which the Hezbollah and the Qods Force provided to the IRGC’s terrorist allies operating in Afghanistan and Iraq—and all of which was used to target to kill and injure Americans, including Plaintiffs.

54. As long-term strategic partners with one another who worked closely together in Iran, ZTE and Huawei (alongside co-conspirator MTN) all understood their counterparties were notorious terrorist fronts used to raise money and source weapons for the Qods Force, Hezbollah, and their proxies in places like Afghanistan and Iraq. Defendants knew or were willfully blind to the fact that their “business” with terrorist front counterparties was serving the terrorists’ ends but proceeded in any event.

55. Hezbollah, the Qods Force, and Regular IRGC, used the IRGC’s relationships with ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN) to optimize Iran’s terrorist enterprise by bolstering the financial and technical capacities of Iran’s terrorist proxies in Afghanistan and Iraq.

56. Through the IRGC’s, including Hezbollah’s and the Qods Force’s, transactions with ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN), Hezbollah, the Qods Force, and the IRGC’s terrorist proxies were able to evade the international sanctions regime to source weapons and weapons components for terror, modernize their communications systems to better encrypt signals traffic, improve their surveillance and intelligence capabilities, and generate tens of millions in annual revenue to fund attacks – all of which Hezbollah, the Qods Force, and the IRGC’s proxies in Afghanistan, including al-Qaeda and the Taliban, used to attack Americans in Afghanistan from 2012 through 2017.

57. The total value of the money, technology, and services that Hezbollah, the Qods Force, and Regular IRGC obtained via ZTE Corp.'s and Huawei Co.'s (alongside their co-conspirator MTN's) business with the IRGC collectively extracted likely ranges into the hundreds of millions of U.S. Dollars in cash and cash equivalents—and the terrorists used those resources to pay for terrorist proxy attacks in Afghanistan and Iraq. The IRGC facilitated violence by all, fueled by Defendants' aid.

58. But this case is not just about money; the technology that ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN) provided to the IRGC, which inevitably flowed through to IRGC proxies al-Qaeda and the Taliban, was uniquely important to the terrorists, enabling them to inflict maximum damage because, among other things, it allowed them to spy on Americans, avoid detection, clandestinely communicate, build and detonate more effective bombs, and develop more accurate and lethal rockets. And on top of the money and the technology, Defendants also provided substantial ongoing logistical and operational aid for the IRGC's, including its Hezbollah Division's and Qods Force's, terrorist enterprise.

59. This is not a case about one or two alleged rogue employees who engaged in a frolic and detour that resulted in a company's money reaching terrorists. Here, each Defendants' executives were thoroughly implicated in the terrorist finance and logistics scheme, and actively supported doing business with known terrorist fronts.

60. Indeed, MTN's leadership even mocked those who raised concerns about the risks of becoming joint venture partners with two notorious Iranian terror fronts: When queried by investors about the "risk of doing business with Iran," MTN's then-CEO "laughed off" such questions, joking that "[MTN] hadn't budgeted for bomb shelters or anything like that."

61. ZTE's executives were similarly culpable. According to the then-Acting Assistant Attorney General, Mary B. McCord, "ZTE engaged in an elaborate scheme to acquire U.S.-origin items, send the items to Iran and mask its involvement in those exports," and the plea agreement ZTE signed on behalf of itself and its subsidiaries "alleges that the highest levels of management within the company approved the scheme."

62. Huawei is much the same. Acting U.S. Attorney for the Eastern District of New York Nicole Boeckmann announced a deferred prosecution agreement by Huawei Co's CFO wherein she "[took] responsibility for her principal role in perpetrating a scheme to defraud a global financial institution," and admitted in the related statements of facts that she had "while acting as the Chief Financial Officer for Huawei, . . . made multiple material misrepresentations to a senior executive of a financial institution regarding Huawei's business operations in Iran" and that she and "her fellow Huawei employees engaged in a *concerted effort to deceive global financial institutions, the U.S. government and the public about Huawei's activities in Iran.*"

63. In August 2021, America withdrew from Afghanistan. A well-organized, cohesive, and integrated Taliban seized the country. Tens of thousands of Afghan heroes fled everyone and everything they knew, for a new life in the U.S.

64. Defendants' business partners and their "Iranian Shareholders" celebrated the terrorists' victory (undoubtedly joined, as discovery is likely to reveal, by many of ZTE's and Huawei's (alongside co-conspirator MTN's) non-U.S. employees and management).

65. ZTE's and Huawei's (alongside co-conspirator MTN's) transactions, and the terrorist attacks they funded, were acts of "international terrorism." 18 U.S.C. § 2333(a).

66. The al-Qaeda/Taliban attacks against Plaintiffs were "planned," "authorized," and jointly "committed" by al-Qaeda, 18 U.S.C. § 2333(d)(2).

67. Plaintiffs are U.S. citizens, and their family members, who served in Afghanistan between 2012 and 2017, and who were killed or wounded in terrorist attacks committed by the IRGC's terrorist proxies in Afghanistan, with material support from the IRGC. As alleged below, Plaintiffs are entitled to recover for their injuries under the federal Anti-Terrorism Act. MTN Group, ZTE, and Huawei are liable under the ATA, 18 U.S.C. § 2333(d)(2), because they aided and abetted the campaign by Hezbollah, the Qods Force, al-Qaeda, and the Taliban, including its Haqqani Network, to commit terrorist attacks in Afghanistan that were committed, planned, or authorized by al-Qaeda.

68. Each Plaintiff was killed or injured by a terrorist attack committed by terrorists who received direct funding, weapons, weapons components, communications technology, and/or operational support made possible by ZTE's and Huawei's conduct.

DEFENDANTS

A. The ZTE Defendants

69. On information and belief, Defendant ZTE Corporation ("ZTE Corp.," together with its subsidiaries, "ZTE"), is a Chinese corporation with a principal place of business located at ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Guangdong Province, People's Republic of China 518057.

70. Defendant ZTE (USA), Inc. ("ZTE USA") is a New Jersey Corporation that is a wholly-owned subsidiary of ZTE Corp., headquartered and authorized to do business at 2425 North Central Expressway, Suite 323, Richardson, Texas, 75080. On March 7, 2017, ZTE and its subsidiaries (including, on information and belief, ZTE USA) entered into a settlement agreement with the U.S. Department of the Treasury's Office of Foreign Assets Control (the "ZTE 2017 OFAC Settlement"). Therein, ZTE USA admitted, *inter alia*, (a) it knowingly participated in a scheme with ZTE Corp. to illegally transfer over \$39 million in U.S. goods to

Iran, and otherwise (b) conducts business for ZTE Corp. on its behalf. For these reasons, allegations regarding “ZTE” in this Complaint apply equally to ZTE USA, because ZTE USA was instrumental in the scheme alleged herein by ZTE generally.

71. Defendant ZTE (TX) Inc. (“ZTE TX”) is a wholly-owned subsidiary of ZTE Corp. ZTE TX is a corporation organized and existing under the laws of the State of Texas with its principal place of business in California at 1900 McCarthy Boulevard, #420, Milpitas, California 95035. As a subsidiary of ZTE, ZTE TX also was party to the ZTE 2017 OFAC Settlement. In the ZTE 2017 OFAC Settlement, ZTE TX admitted, *inter alia*, (a) it knowingly participated in a scheme with ZTE Corp. to illegally transfer over \$39 million in U.S. goods to Iran and otherwise (b) conducts business for ZTE Corp. on its behalf. For these reasons, allegations of acts after ZTE TX’s formation regarding “ZTE” in this Complaint apply equally to ZTE TX, because ZTE TX was instrumental in the scheme alleged herein by ZTE generally.

B. The Huawei Defendants

72. On information and belief, Defendant Huawei Technologies Co., Ltd. (“Huawei Co.,” together with its subsidiaries and affiliates, “Huawei”) is a Chinese company with a principal place of business located at Huawei Industrial Base, Bantian Street, Longgang District, Shenzhen, Guangdong Province, People’s Republic of China 518129. Huawei Co. is owned by its parent company Huawei Investment & Holding Co., Ltd. (“Huawei Holdings”), a Chinese company registered in Shenzhen, Guangdong, People’s Republic of China.

73. Defendant Huawei Technologies USA Inc. (“Huawei USA”) is a corporation organized under the laws of the State of Texas with its principal place of business in Texas at 16479 Dallas Parkway, Suite 355, Addison, Texas 75001. Huawei USA is a wholly-owned indirect subsidiary of Huawei Co.

74. Defendant Huawei Device USA Inc. (“Huawei Device USA”) is a Texas corporation that is organized under the laws of the State of Texas with its principal place of business in Texas at 16479 Dallas Parkway, Suite 355, Addison, Texas 75001. Huawei Device USA is a subsidiary of Huawei Co. and Huawei Co.’s parent, Huawei Holdings.

75. Defendant Futurewei Technologies, Inc. (“Futurewei”) is a corporation organized under the laws of the State of Texas with its principal place of business in California at 2220 Central Expressway, Santa Clara, California 95050. Futurewei is a subsidiary of Huawei Co. and Huawei Co.’s parent, Huawei Holdings.

76. Defendant Skycom Tech Co., Ltd. (“Skycom”) is a corporation registered in Hong Kong with its principal place of business located in Iran at No. 114 Corner of Kordestan Highway, Tehran, Iran. As of 2007, Skycom was wholly-owned by Huawei Co.’s subsidiary Hua Ying (“Hua Ying”). In November 2007, Huawei Co. directed Hua Ying to transfer its shares in Skycom to Calicula Holdings Ltd. (“Calicula”), another a subsidiary controlled by Huawei Co.

JURISDICTION AND VENUE

77. This Court has subject-matter jurisdiction under 18 U.S.C. § 2338 and 28 U.S.C. § 2331.

78. This Court has personal jurisdiction over each of the Defendants under Federal Rule of Civil Procedure 4(k)(1)I and/or 4(k)(2), and 18 U.S.C. § 2334(a).

79. ZTE’s acts in the United States, including but not limited to obtaining U.S.-origin technology and equipment for export to Iran, including but not limited to working with and through, ZTE USA and ZTE TX to do so, and targeting the United States, including by entering into transactions with fronts, operatives, and agents for the Hezbollah, the Qods Force, and

Regular IRGC that were intent on harming United States nationals in Afghanistan, make appropriate this Court's jurisdiction over ZTE Corp., ZTE USA, and ZTE TX.

80. ZTE does business in New York, including by selling cell phones and telecommunications equipment. ZTE USA is registered to do business in the state of New York, and its Registered Agent is Incorp Services Inc. of Albany, NY. ZTE also maintains accounts with financial institutions, located in New York, which, on information and belief, ZTE utilized in furtherance of their scheme alleged herein. Additionally, the U.S. Attorney's Office for the Southern District of New York is currently investigating ZTE with regard to potential bribes paid by ZTE, and on information and belief the conduct being investigated occurred in New York. ZTE has consistently, during the relevant time period, entered into major partnership and business deals in New York, and typically announces new product offerings at events physically in New York. When ZTE entered into a partnership with the New York Knicks, Lixin Cheng, ZTE USA's then CEO said that New York was a community "in which we live and work." Further, ZTE entered into other key partnership with counterparties in New York necessary for ZTE to obtain the devices and technology that its IRGC-front counterparties sought (and which ZTE delivered). Specifically, ZTE entered into an agreement with a counterparty in New York to source rugged glass fronts for their cell phones, which was necessary for the rough physical environments in which the terrorists operate and entered into another agreement with a counterparty in New York that assisted ZTE with enhancing the security features on its smartphones, which was necessary for the terrorists to be able to avoid detection and operate without surveillance.

81. Huawei's acts in the United States, including but not limited to, obtaining U.S.-origin services, technology, and equipment for export to Iran, working with and through

Skycom, Futurewei, Huawei Device USA, and Huawei USA to do so, and targeting the United States, including by entering into transactions with fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC that were intent on harming United States nationals in Afghanistan, make appropriate this Court's jurisdiction over Huawei Co., Huawei USA, Futurewei, Huawei Device USA, and Skycom.

82. Huawei does business in New York, including by selling cell phones and telecommunications equipment. Huawei also maintains accounts with financial institutions, located in New York, which, on information and belief, Huawei utilized in furtherance of their scheme alleged herein. Additionally, the U.S. Attorney's Office for the Eastern District of New York is currently pursuing criminal charges against Huawei, including its American subsidiaries Futurewei and Huawei Device USA, for, *inter alia*, their unlawful conduct, relating to their Iranian business interests, including conduct in the Eastern District of New York.

83. Defendants' co-conspirators, MTN Irancell's and MTN Group's (inclusive of their officers', directors', employees', and agents') acts in the United States, including but not limited to obtaining U.S.-origin technology and equipment for export to Iran, and targeting the United States, including by entering into transactions with fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC that were intent on harming United States nationals in Afghanistan, also make appropriate this Court's jurisdiction over Defendants as acts in furtherance of the same conspiracy to which Defendants agreed to participate.

84. Defendants' co-conspirators, MTN Group and MTN Irancell (though MTN Group and/or MTN Dubai as "orbits" or buffers for MTN Irancell), do business in New York, including by procuring U.S.-origin goods and services from companies located in the U.S., including New York, for the IRGC's, including Hezbollah's and the Qods Force's, fronts, agents, and

operatives, maintaining accounts with financial institutions located in New York, including, on information and belief, a loan facility with Citibank and a depository account with the Bank of New York, using the New York-based financial system and banks to manage cash flow for MTN Group, MTN Irancell, and MTN Dubai, utilizing a bank account in New York to wire funds to an agent of the IRGC to consummate a bribe relating to MTN's acquisition of the Irancell license, and working with a New York-based financial institution to issue a sponsored American depository receipt (ADR).

85. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

I. SINCE THE ISLAMIC REVOLUTION IN 1979, THE ISLAMIC REVOLUTIONARY GUARD CORPS, OR IRGC, HAS FOMENTED AND SUSTAINED ANTI-AMERICAN TERRORISM

86. The 1979 Iranian Revolution was fueled in large part by militant anti-Americanism. Eliminating the United States' role in the geographic region surrounding Iran – including through violence – was and remains a central tenet of Iranian foreign policy. Since the Iranian Revolution, Iran has engaged in and supported acts of terrorism directed at the United States and its allies as an instrument of Iran's foreign policy.

87. Iran's support of terrorist proxies like Hezbollah, Hamas, al-Qaeda, and the Taliban, including its Haqqani Network,³ is well-documented. Iran's support for such groups is especially prevalent in areas where Iran abstains from open conflict. As a result of Iran's consistent and longstanding support of anti-American terrorism, the U.S. State Department

³ The Haqqani Network is a part of the Taliban. In this complaint, every reference to "Taliban" also includes the Haqqani Network.

formally designated Iran as a State Sponsor of Terrorism in 1984. It has maintained that designation at all times since. In 2007, the U.S. State Department described Iran as “the most active state sponsor of terrorism” in the world and “a threat to regional stability and U.S. interests in the Middle East because of its continued support for violent groups.”

88. Iran is politically and ideologically hostile to the United States and its allies. Enmity toward America is foundational for the Iranian regime in general, and most of all, for Grand Ayatollah Khamenei, who is the effective leader of the Islamic Revolutionary Guard Corps, including its Hezbollah Division and Qods Force, both of which report to him personally as head of the IRGC.⁴ At a 2005 rally, Khamenei explained, “Our people say ‘Death to America,’ and this is like the saying ‘I seek God’s refuge from the accursed Satan,’ which is recited before any chapter of the Koran, even before ‘In the name of Allah the Compassionate, the Merciful.’” Khamenei said the routine chanting of “Death to America” is designed so that Iranians “will never forget, even for a moment, that Satan is ready to attack him. . . . The saying ‘Death to America’ is for this purpose.”⁵

A. Islamic Revolutionary Guard Corps

89. Iran carries out its support of terrorism largely through the IRGC.

90. The IRGC “has a relatively strict command-and-control protocol and answers directly to the Supreme Leader, Ayatollah Ali Khamenei.” The Supreme Leader serves as head of the IRGC and routinely employs the IRGC to further Iran’s global terrorist agenda.

⁴ The IRGC is comprised of the Hezbollah Division, more popularly known as Lebanese Hezbollah or Hezbollah, the Qods Force, and the Regular IRGC. In this complaint, every reference to “IRGC” also includes Hezbollah, the Qods Force, and the Regular IRGC

⁵ Ali Khamenei, Channel 1, Iranian TV (Mar. 14, 2005).

91. As the U.S. Treasury Department noted in 2010 when it designated certain IRGC officials pursuant to Executive Order 13224, “Iran also uses the . . . IRGC . . . to implement its foreign policy goals, including, but not limited to, seemingly legitimate activities that provide cover for intelligence operations and support to terrorist and insurgent groups.”

92. The IRGC was established to safeguard the revolution, meaning, to pursue violence inside of Iran, i.e., terrorism against its own people, and external to Iran, i.e., terrorism against the United States and Israel, whom the IRGC considered to be the “Great Satan” and “Little Satan,” respectively. As Monika Gill, a defense researcher, explained in an analysis published by NATO in 2020: “The aphorism that ‘war made the state and the state made war’ applies to the IRGC; war made the Guard and the Guard made war.”⁶

93. In her analysis of MTN Irancell, as published by NATO, Ms. Gill explained that under the IRGC’s official, publicly communicated security doctrine, the IRGC’s “security” interests are defined as “leading an ongoing resistance” in a zero-sum fight the United States:

[T]here is a strong feeling of shared Shi’a victimhood driving the IRGC worldview. Ayatollah Khomeini in particular, held the view ... This sense of being surrounded by enemies of Iran and therefore, enemies of Shi’ism pervades the strategic narrative of both the neoconservative clerical establishment and the IRGC. Paradoxically, the IRGC’s strategic narrative is well served by maintaining enemies and continually reinforcing the notion that the Islamic Republic is under attack. It allows the IRGC to define Iran in *diametric opposition to the enemies of the revolution* and to profess that it is *leading an ongoing resistance*. In this view, the IRGC strategic narrative is a *narrative of resistance*, expressing defiance against threats to the revolution, externally imposed hard and soft war, and the enemies of the Iranian state.⁷

⁶ Monika Gill, *Capitalism, Communications, and the Corps: Iran’s Revolutionary Guard and the Communications Economy*, Defence Strategic Communications: The Official Journal of the NATO Strategic Communications Centre of Excellence, at 97 (Autumn 2020) (“Gill, *Capitalism, Communications, and the Corps*”).

⁷ Gill, *Capitalism, Communications, and the Corps* at 97 (emphasis added). Indeed, MTN Irancell’s CEO publicly aligned MTN Irancell with the IRGC’s “resistance” narrative and admitted that Irancell serves the IRGC’s terrorist “resistance” efforts as part of its corporate

94. As a result of the IRGC's consistent and longstanding support of anti-American terrorism, Iran was designated as a State Sponsor of Terrorism on January 19, 1984, pursuant to section 6 of the Export Administration Act of 1979 (50 U.S.C. § 4605), section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. § 2371), and section 40 of the Arms Export Control Act (22 U.S.C. § 2780). The United States has maintained that designation at all times since.

95. On October 29, 1987, President Ronald Reagan issued Executive Order 12613 based upon his finding "that the Government of Iran is actively supporting terrorism as an instrument of state policy," and also as a result of Iran's "aggressive and unlawful military action against U.S.-flag vessels." Exec. Order 12813, 52 Fed. Reg. 4194D (Oct. 30, 1987).

96. In 1990, the IRGC transferred activities outside of Iran to its subordinate branch, the Qods Force, which translates to "Jerusalem Force," in reference to the IRGC's desire to destroy the state of Israel and take back Jerusalem.

97. On March 15, 1995, President Clinton announced that "the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security ... of the United States. ..." Exec. Order 12957, 60 Fed. Reg. 14615 (Mar. 17, 1995).

"social responsibility." ICTNA (Iran), *Irancell Brings 4G to Iran* (Nov. 22, 2014) (MTN Irancell CEO, Dezfouli, stated, among other things, that Irancell's "development" of communications technology "will make some of the objectives pursued by the resistive economy come true: Bringing about agility and dynamism and developing the macro indexes; Resistance against the threatening elements; Resorting to the local capacities; An approach of ever-increasing efforts; Public-centricity; Safety of the strategic and basic goods; Reducing the dependency to the oil; Changing the Consumption Pattern; Combat against corruption and Becoming more knowledge-centered" and that "Sponsoring sports teams, supporting the State Welfare Organization, Building schools in impoverished regions and cooperation with Imam Khomeini Relief Foundation were among other measures taken by Irancell for fulfilling its social responsibilities."), <https://www.ictna.ir/id/065513/>.

98. On August 21, 1997, President Clinton issued Executive Order 13059 to consolidate and clarify Executive Orders 12957 and 12959, and comprehensively prohibit trade intended to benefit, among other things, the IRGC, including its Hezbollah Division and Qods Force. Exec. Order 13059, 62 Fed. Reg. 44531 (Aug. 21, 1997). (That same year, the U.S. also designated Iran’s lead terror agent, Hezbollah, as an FTO.)

99. In 1998, Brigadier General Qassem Soleimani was appointed head of the Qods Force, a role in which he served continuously until his death in a U.S. airstrike in 2020.

100. The Department of Treasury implemented regulations pursuant to these Executive Orders which, in general, broadly prohibit any economic transactions with any entities that are controlled by the Government of Iran. 31 C.F.R. § 560.304 (defining “Government of Iran”), 31 C.F.R. § 560.313 (defining “entity owned or controlled by the Government of Iran”); 31 C.F.R. § 560.314 (defining “United States person”).

101. In 2007, the U.S. State Department described Iran as “the most active state sponsor of terrorism” in the world and “a threat to regional stability and U.S. interests in the Middle East because of its continued support for violent groups.”⁸

102. On May 27, 2009, the U.S. Treasury Department announced additional IRGC-related sanctions further reflecting the long-standing U.S. conclusion that the IRGC used its revenue to pay for Hezbollah’s operations and training activities:

The U.S. Department of the Treasury [] designated ... two Africa-based supporters of the Hizballah terrorist organization, under E.O. 13224. E.O. 13224 targets ***terrorists and those providing support to terrorists or acts of terrorism*** by ... prohibiting U.S. persons from engaging in any transactions with them.

“We will continue to take steps to protect the financial system from the threat posed by ***Hizballah and those who support it***,” said Under Secretary for Terrorism and Financial Intelligence Stuart Levey. ... Iran ... provide[s]

⁸ U.S. State Dep’t, *Country Reports on Terrorism 2007* at 172 (Apr. 2008).

significant support to Hizballah, giving money, weapons and training to the terrorist organization. In turn, Hizballah is closely allied with and has an allegiance to [Iran]. ***Iran is Hizballah's main source of weapons and uses its Islamic Revolutionary Guard Corps to train Hizballah operatives in Lebanon and Iran.*** Iran provides hundreds of millions of dollars per year to Hizballah.⁹

103. The IRGC has a long and well-documented history of assassinations, kidnappings, bombings, and arms dealing. It also regularly trains foreign terrorist proxies whose attacks promote Iran's political goals, often working side-by-side with Hezbollah.

104. The IRGC has used Hezbollah and its proxies to commit terrorist attacks. While it is a Lebanese-based terrorist group, Hezbollah has pledged fealty to Iran's Supreme Leader. Each year the IRGC provides Hezbollah approximately \$100 million to \$200 million in funding and weapons. As Ali Akbar Mohtashemi (a Hezbollah founder, former Iranian ambassador to Syria and Lebanon, and former Iranian Minister of Interior) explained, "[Hezbollah] is part of the Iranian rulership; [Hezbollah] is a central component of the Iranian military and security establishment; the ties between Iran and [Hezbollah] are far greater than those between a revolutionary regime with a revolutionary party or organization outside its borders."¹⁰

105. On April 15, 2019, the U.S. State Department designated the Regular IRGC and the Qods Force as a Foreign Terrorist Organization,¹¹ which completed the designation of every IRGC-related entity as an FTO.¹² Announcing the designation, President Trump explained that

⁹ Press Release, U.S. Treasury Dep't, *Treasury Targets Hizballah Network in Africa* (May 27, 2009) (emphases added).

¹⁰ *Killing Americans and Their Allies*.

¹¹ See 84 Fed. Reg. 15,278-01 (Apr. 15, 2019).

¹² In 1997, the State Department designated Hezbollah – known to the IRGC as its own Hezbollah Division – as an FTO.

“the IRGC *actively participates in, finances, and promotes terrorism as a tool of statecraft*.”¹³

According to the U.S. State Department’s public statement explaining the designation, Hezbollah, the Qods Force, and Regular IRGC have “been directly involved in terrorist plotting; its support for terrorism is *foundational and institutional*, and it has killed U.S. citizens.”¹⁴ Through the IRGC’s, including Hezbollah’s and the Qods Force’s, support for terrorist organizations throughout the region, “[t]he Iranian regime has made a clear choice not only to fund and equip, but also to fuel terrorism, violence, and unrest across the Middle East.”¹⁵

106. When the State Department designated the IRGC as a Foreign Terrorist Organization, Secretary of State Michael R. Pompeo stated, among other things:
- (i) “This is the first time that the United States has designated a part of another government as an FTO. ... *[T]he Iranian regime’s use of terrorism as a tool of statecraft makes it fundamentally different from any other government.* ... “
 - (ii) “For 40 years, the [IRGC] has actively engaged in terrorism and created, supported, and directed other terrorist groups. The IRGC ... regularly violates the laws of armed conflict; it plans, organizes, and executes terror campaigns all around the world. ...”
 - (iii) “The IRGC institutionalized terrorism shortly after its inception, directing horrific attacks against the Marine barracks in Beirut in 1983 and the U.S. embassy annex in 1984 alongside *the terror group it midwifed, Lebanese Hizballah*. Its operatives have worked to destabilize the Middle East ...”
 - (iv) “Our designation makes clear ... that [the] Iranian regime not only supports terrorist groups, but engages in terrorism itself. This designation also brings unprecedented pressure on figures who lead the regime’s terror campaign, individuals like Qasem Soleimani. ... He *doles out the regime’s profits to terrorist groups across the region and around the world.*”¹⁶

¹³ Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization (Apr. 8, 2019) (emphasis added).

¹⁴ U.S. State Dep’t, *Fact Sheet: Designation of the Islamic Revolutionary Guard Corps* (Apr. 8, 2019) (emphasis added).

¹⁵ *Id.*

¹⁶ Secretary of State Michael R. Pompeo, U.S. Department of State, *Remarks to the Press* (Apr. 8, 2019) (emphasis added).

107. As the world’s worst sponsor of terrorism, the Iranian regime was unique. It was not a “normal” government, but a regime that facilitated a climate where Hezbollah, the Qods Force, and the Regular IRGC relied upon the IRGC’s corporate allies to directly enable violence in an open and shocking manner. As Ambassador Mark D. Wallace, the CEO of United Against Nuclear Iran (“UANI”), explained, “[i]nternational organizations must also realize that their relationship with Iran is not just ... ‘business as usual,’ ... Put bluntly, Iran is in violation of many of its international treaty obligations, and it *should not be treated like a member in good standing* of international bodies.”¹⁷

B. Hezbollah

108. Hezbollah, translated as “Party of God,” “first emerged as a militia in opposition to the 1982 Israeli invasion of Lebanon.”¹⁸

109. “Although Iran was engaged in the Iran-Iraq War at the time of the Israeli occupation, Iran’s Islamic Revolutionary Guard Corps (IRGC) took the lead in organizing, training, and equipping Hezbollah.”¹⁹

110. “To this end, Syria allowed 2,500 members of the IRGC to enter Lebanon and set up training camps among the Shi’ite population in the Beqa’a Valley ... Training at the IRGC camps became a prerequisite for membership in Hezbollah.”²⁰

¹⁷ Statement of the Honorable Mark D. Wallace, CEO United Against Nuclear Iran before the U.S. House of Representatives Committee on Foreign Affairs, *Iran Sanctions*, Congressional Testimony via FDCH (May 17, 2012) (emphasis added), 2012 WLNR 10405070 (“Wallace May 17, 2012 Testimony”).

¹⁸ Marc Lindemann (Captain, New York National Guard), *Laboratory of Asymmetry: The 2006 Lebanon War and the Evolution of Iranian Ground Tactics*, Military Review (May 1, 2010), 2010 WLNR 28507137 (“Lindemann, *Laboratory of Asymmetry*”).

¹⁹ Lindemann, *Laboratory of Asymmetry*.

²⁰ *Id.*

111. The IRGC created Hezbollah as a subordinate part of the IRGC known as the “Hezbollah Division.”²¹

112. Hezbollah likewise considers itself a part of the IRGC. In 1985, “Hezbollah publicly acknowledged its reliance on Iran,”: “We view the Iranian regime as the vanguard and new nucleus of the leading Islamic State in the world. We abide by the orders of one single wise and just leadership, represented by ‘*Wali Faqih*’ [rule of the jurisprudent] and personified by Khomeini.”

113. Hezbollah operatives swear a personal oath of loyalty to Iran’s Supreme Leader, Ayatollah Khamenei, and personally pledge to carry out their terrorist missions in his name.

114. The IRGC directly funds its Hezbollah Division in the same manner as its Qods Force, as they are two sides of the same IRGC external terror coin. As the Defense Intelligence Agency (“DIA”) concluded with “high confidence” in 2010, “Iran has methodically cultivated a network of sponsored terrorist surrogates capable of conducting effective, plausibly deniable attacks against ... the United States,” and the DIA “judge[d]” that “Tehran provide[d] support to terrorist and militant groups to support Iran’s strategic interests in each situation.”²²

115. DIA concluded: “[e]lements of Iran’s Islamic Revolutionary Guard Corps []have provided direct support to terrorist groups, assisting in the planning of terrorist acts or enhancing terrorist group capabilities.”²³

²¹ Michael Knights, *The Evolution of Iran’s Special Groups in Iraq*, Combating Terrorism Center at West Point, CTC Sentinel, Vol. 3, No. 11 (Nov. 2010) (“Knights, *The Evolution of Iran’s Special Groups in Iraq*”).

²² Defense Intelligence Agency, *Unclassified Report on Military Power of Iran* (Apr. 2010).

²³ *Id.*

116. Articles 150 and 154 of the Iranian Constitution order the IRGC to export Iran’s Islamic Revolution and aiding insurgents. Under Article 150, the IRGC is responsible for “guarding the revolution and its achievements,” (meaning, exporting the Islamic Revolution),²⁴ and Article 154 confirms that Iran “supports the just struggles of the *mustad’afun* [downtrodden] against the *mustakbirun* [oppressors] in every corner of the globe.” Thus, Iran’s constitution directly embraces proxy terror (“the just struggles of the downtrodden”) targeting the United States (i.e., “against the oppressors”).²⁵

117. On January 25, 1995, the United States designated Hezbollah as a Specially Designated Terrorist.

118. On October 8, 1997, the United States designated Hezbollah as an FTO, and it has retained that designation ever since.

119. Richard Armitage, the Deputy Secretary of State under President George W. Bush, has described Hezbollah as “the ‘A-Team of Terrorists,’ ”²⁶ and former CIA director George Tenet has opined that Hezbollah “is [al-Qaeda’s] equal if not far more capable

²⁴ Under Iran’s revolutionary doctrine, the Iranian government posits that it must always remain on the attack with respect to its promotion of insurgents against the Great Satan because, if Iran were to fall back (according to this paranoid theory), the U.S. would overrun Iran. Consequently, inside Iran and around the world, people familiar with Iran and the IRGC understand that references to “guarding the revolution” are *not* defensive, but rather, are *offensive* because, under the paranoid Iranian view, the only way to “guard the revolution” is to go on the attack outside of Iran, through proxy terror campaigns. Any suggestion to the contrary is, quite literally, IRGC terrorist propaganda.

²⁵ When the Iranian government references “the oppressors” without any specification as to whom, that *exclusively* means only two countries: the United States and Israel. This is so because the Iranian regime was founded in direct opposition us and our ally, and Iran’s founding documents mention no other hostile actor beyond the U.S. and Israel. Any suggestion to the contrary is, literally, Iranian propaganda designed for a western audience.

²⁶ Ed Bradley, *Hezbollah: “A-Team of Terrorists”*, CBS News (Apr. 18, 2003).

organization.”²⁷ For example, Hezbollah’s chief terrorist mastermind, Mugniyeh, originally instructed al-Qaeda in the suicide bombing tactic.

120. Hezbollah was and is the IRGC’s, including the Qods Force’s, lead terrorist proxy in Iraq and the broader Middle East, serving, in effect, as the IRGC’s external terrorist operations arm in conjunction with Hezbollah’s close ally and patron, the Qods Force.

121. Hezbollah’s activities have stretched far beyond Lebanon’s borders. Hezbollah’s primary stated goal is the destruction of the United States and Israel, which it calls the “Great Satan” and the “Little Satan,” respectively.²⁸ Hezbollah also frequently functions as a terrorist proxy for the IRGC, committing and orchestrating terrorist attacks abroad with the IRGC’s, including the Qods Force’s, support. Hezbollah’s 1985 manifesto proclaims that the “first root of vice is America” and explains that “Imam [Ruhollah] Khomeini, our leader, has repeatedly stressed that America is the cause of all our catastrophes and the source of all malice.”²⁹ In 2003, Hezbollah Secretary-General Hassan Nasrallah proclaimed: “Let the entire world hear me. Our hostility to the Great Satan [America] is absolute Regardless of how the world has changed after 11 September, Death to America will remain our reverberating and powerful slogan: Death to America.”³⁰

²⁷ *Current and Future Worldwide Threats to the National Security of the United States: Hearing Before the S. Comm. on Armed Services*, 108th Cong. 60 (Feb. 12, 2003) (testimony of George J. Tenet).

²⁸ See Times of Israel, *Nasrallah Proud that PM, Obama Discussed Hezbollah* (Nov. 11, 2015); Ariel Ben Solomon, *Nasrallah ‘Proud’ that Netanyahu and Obama Discussed Hezbollah in White House Meeting*, Jerusalem Post (Nov. 11, 2015).

²⁹ Hezbollah Manifesto, *reprinted in Anti-American Terrorism and the Middle East: A Documentary Reader* 50 (Barry Rubin & Judith Colp Rubin eds., Oxford Univ. Press 2002).

³⁰ Sept. 27, 2002 Al-Manar broadcast, *quoted in* “Hassan Nasrallah: In His Own Words,” Committee for Accuracy in Middle East Reporting in America (July 26, 2006).

122. Hezbollah has coordinated terrorist attacks around the world primarily by acting through terrorist proxies. As Dr. Matthew Levitt has explained, “Hezbollah is extremely adept at recruiting members from local populations in areas where they have networks on the ground.”³¹ Hezbollah has trained and equipped these local terrorist proxies to carry out terrorist attacks on Hezbollah’s behalf. Hezbollah has successfully employed this strategy to facilitate attacks by its proxies in (among other places) Paris, France (1985-86); Buenos Aires, Argentina (1992); and Khobar, Saudi Arabia (1996).

123. Hezbollah is, and has always been widely understood in the U.S., Europe, Middle East, and Asia to be Iran’s purpose-built anti-American and anti-Israeli Arabic Shiite terrorist division, which the IRGC designed to integrate within the IRGC’s terror architecture, including, but not limited to, its financial, operational, and logistics networks in order to ensure that Hezbollah was inseparable from the Regular IRGC and Qods Force and always remained a formal part of the IRGC. The IRGC built Hezbollah this way because the IRGC wanted to be able to control Hezbollah’s every move while simultaneously maintaining the fiction that Hezbollah were merely “resistance” fighters. The IRGC’s ploy was key to facilitating its worst terrorist plots because the IRGC’s primary purpose when it created its Hezbollah Division was to secure the IRGC’s plausible deniability on a structural level by interposing a buffer – Hezbollah – between the IRGC and the Americans whom the IRGC wanted to murder.

124. The IRGC has long relied on Hezbollah to aid the Qods Force’s efforts to supply al-Qaeda and its Taliban allies,³² as they targeted Americans in Afghanistan and Iraq:

³¹ Matthew Levitt, *Hezbollah: A Case Study of Global Reach*, Remarks to a Conference on “Post-Modern Terrorism: Trends, Scenarios, and Future Threats” at 4 (Sept. 8, 2003).

³² The IRGC was essential to enabling trans-Sunni Islamist cooperation between Afghanistan/Pakistan and Iraq and maximizing the ability of al-Qaeda and Taliban terrorists in

- (i) The IRGC has relied upon Hezbollah and the Qods Force to aid attacks against Americans by al-Qaeda and its allies since the early 1990s (in the case of al-Qaeda and Ansar al-Islam) and/or shortly after 9/11 (in the case of the Taliban).
- (ii) Before 9/11, the IRGC, al-Qaeda, the Taliban, and their respective affiliates, worked together to broker combined Islamist terrorist training activities at Taliban sites in Afghanistan, during which time terrorists from Hezbollah, the Qods Force, al-Qaeda, the Taliban, Hamas, and Palestinian Islamic Jihad trained, prayed, and studied together in order to develop the long-term skills and relationships that bin Laden demanded under his corporate “always be closing” model of terror, which emphasized cross-pollination with every possible Islamist terrorist group as long as such group wanted to help al-Qaeda and its allies kill Americans.³³
- (iii) After 9/11, al-Qaeda, the IRGC, and their respective affiliates, intensified their transnational terrorist alliance; the IRGC acted primarily through its Hezbollah and Qods Force operatives distributed in cells worldwide, while al-Qaeda and the Taliban, including its Haqqani Network, for their part, acted primarily through al-Qaeda- and Haqqani Network-related “polyterrorists” who served more than one member of the Syndicate, e.g., Sirajuddin Haqqani was a member of al-Qaeda and the Taliban, including its Haqqani Network.

C. Qods Force

125. The U.S. State Department has observed that “Iran used the [Qods Force] to implement foreign policy goals, provide cover for intelligence operations, and create instability in the Middle East. The Qods Force is Iran’s primary mechanism for cultivating and supporting

Afghanistan to leverage the personnel, funding streams, resources, and trainers available in Iraq in order to enhance the lethality of al-Qaeda and Taliban attacks in Afghanistan (and vice versa). For example, al-Qaeda relied upon the funding and logistical support provided by the IRGC to source CAN fertilizer from Pakistan (to use for bombs in Afghanistan and Iraq), secure cell phones from America (to be used for communications or as a cash equivalent “free good” valued at \$2,000 per phone), and narcotics trafficking and laundering assistance, which funded al-Qaeda’s and the Taliban’s attacks against Americans in Afghanistan, including those that injured Plaintiffs and their loved ones.

³³ See, e.g., Hal Bernton, Mike Carter, David Heath and James Neff, *Going To Camp*, Seattle Times (Aug. 4, 2002) (“By [1998], al-Qaida training was formalized. There was even a textbook, available in Arabic, French and other languages. ... Trainees practiced with small arms, assault rifles and grenade launchers provided by the Taliban They learned about explosives and land mines. Representatives of terrorist groups, including Hamas, Hezbollah and Islamic Jihad, gave lectures on their organizations.”), 2002 WLNR 2584645.

terrorists abroad.”³⁴ The Qods Force is the driving force behind Iran’s activities in Afghanistan, as well as in Iraq, Syria, and elsewhere in the Middle East.

126. The Qods Force is responsible to and directed by the Supreme Leader of Iran. Major General Qassem Soleimani was the chief of the Qods Force for more than twenty years and oversaw the Qods Force’s support for Hezbollah and its proxies to promote Iran’s policies throughout the region. Soleimani took his directions from Khamenei, with whom he shared a close personal relationship. Soleimani was killed in a U.S. airstrike in Baghdad, Iraq on January 3, 2020. Khamenei then appointed General Esmail Ghaani to replace Soleimani.

127. The Qods Force provides weapons, funding, and training for terrorist operations targeting American citizens, including for Hezbollah and, through Hezbollah, for IRGC proxies like al-Qaeda and the Taliban. Iran’s Supreme Leader and central government are aware of and encourage those acts. Applying pressure against the United States by funding and supplying Hezbollah and other terrorist proxies in the Middle East and Central Asia is an official component of IRGC policy.

128. The Qods Force has four regional commands, with each focused on implementing Iran’s foreign policy in a neighboring region. The First Corps focuses on Iraq, the Second Corps on Pakistan, the Third Corps on Turkey and Kurdistan, and the Fourth Corps on Afghanistan.

129. The Qods Force’s leader until his death, Qassem Soleimani, infamously boasted about his ability to threaten American lives in Afghanistan by relaying a message, through an intermediary, directly to U.S. General David Petraeus, whom Soleimani taunted: “Dear General Petraeus, You Should know that I, Qassem Soleimani, control the policy for Iran with respect to Iraq, Lebanon, Gaza, and Afghanistan.”

³⁴ U.S. State Dep’t, *Country Reports on Terrorism 2015* at 300 (June 2, 2016).

130. The Qods Force provides weapons, funding, and training for terrorist operations targeting American citizens in Afghanistan, including by supporting terrorist organizations such as the Taliban. As the U.S. government's Joint Improvised Explosive Device Defeat Organization ("JIEDDO") concluded: "Iran's use of weapons smuggling networks is fairly predictable and meant to shape the manner in which foreign countries deal with Iran."³⁵ For that reason, the Qods Force varies the quantity, rate, and types of weapons provided to its proxy terrorist organizations depending on the amount of pressure Iran wants to exert on a particular country. Applying pressure against the United States by funding and supplying terrorist proxies in the Middle East and Central Asia is thus an official component of Iran's foreign policy.

131. The Qods Force operates a broad global network of front companies, often co-located with Hezbollah. Indeed, in recognition of the central role of cover to IRGC doctrine, the IRGC created the Qods Force's Unit 400, which was tasked with the mission of facilitating the IRGC's terrorist finance and logistics activities through illicit commercial transactions conducted by a global network of IRGC fronts.³⁶

132. In October 2007, the U.S. Treasury Department designated the Qods Force as a SDGT under Executive Order 13224 for providing material support to the Taliban and other

³⁵ Eric Parks, *Iranian Weapons Smuggling Activities in Afghanistan* at 9, JIEDDO J2 Open Source Augmentation and Analysis Cell (Sept. 3, 2009) ("*JIEDDO Report*").

³⁶ See, e.g., Shahriar Kia, *Global Terrorist Activities Of The Iranian Mullah Regime*, Weekly Blitz (Bangladesh) (Dec. 4, 2021) ("Unit 400 has a network of facilitators and proxies, including elements in organized crime syndicates. These individuals collect information, make preliminary logistical preparations, and carry out operations if necessary. These individuals sometimes are trained inside Iran and sometimes in the Quds Force's training camps across the globe. Unit 400 has various front companies that both provide cover and money for this terrorist entity to operate. Two companies, Arash Zoobin, and Aria Navid, are used to secretly transfer weapons for Unit 400. Besides, the IRGC uses its vast network of front companies, religious or charitable organizations around the world to recruit facilitators."), 2021 WLNR 39679934.

terrorist organizations, including Hezbollah and terrorist groups in Iraq.³⁷ The U.S. Treasury Department also designated multiple Qods Force members as Specially Designated Nationals pursuant to Executive Order 13224, based on their activities in Afghanistan.³⁸ Announcing the Qods Force’s SDGT-related designations, Treasury confirmed that “[t]he Qods Force”:

- (i) “provide[d] material support to the Taliban, Lebanese Hizballah, Hamas, [and] Palestinian Islamic Jihad”;
- (ii) “[was] the [IRGC’s] primary instrument for providing lethal support to the Taliban”;
- (iii) “provide[ed] weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan”;
- (iv) “support[ed] Hizballah’s military, paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support”;
- (v) “operate[d] training camps for Hizballah in Lebanon” “and” “trained more than 3,000 Hizballah fighters at IRGC training facilities in Iran”;
- (vi) “provide[d] roughly \$100 to \$200 million in funding a year to Hizballah and” “assisted Hizballah in rearming in violation of UN Security Council Resolution 1701”; and
- (vii) “provide[d] lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi’a militants who target[ed] and kill[ed] Coalition [] forces.”³⁹

133. In light of the foregoing, the Treasury Department confirmed, on behalf of the U.S. government, that “[t]hrough Qods Force material support” the United States “believe[d] Iran [was] seeking to inflict casualties on U.S.” “forces” in the Middle East.⁴⁰

134. Moreover, the Treasury Department emphasized that the U.S. government intended the Qods Force’s newly announced SDGT designation to signal to multinational

³⁷ Press Release, U.S. Treasury Dep’t, *Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007).

³⁸ *Id.*

³⁹ *Id.* (emphases added).

⁴⁰ *Id.*

corporations and their C-Suites – like Defendants – that they could no longer do business with the IRGC’s commercial fronts. Among other things, Treasury stated:

- (i) “The U.S. Government is taking [] major actions today to counter Iran’s ... support for terrorism by exposing Iranian ... companies and individuals that have been involved in these dangerous activities and by cutting them off from the U.S. financial system. ... The Treasury Department [] designated the IRGC-Qods Force (IRGC-QF) under E.O. 13224 for providing material support to ... terrorist organizations...”
- (ii) “Last week, [] Treasury [] issued a warning to U.S. banks setting forth the risks posed by Iran.... Today’s actions are consistent with this warning, and provide additional information to help [] institutions protect themselves from deceptive [] practices by Iranian entities and individuals engaged in or supporting ... terrorism.”
- (iii) “As a result of our actions today, all transactions involving any of the designees and any U.S. person will be prohibited ... Today’s designations also notify the international private sector of the dangers of doing business with ... the many IRGC-affiliated companies that pervade several basic Iranian industries. ...”
- (iv) “Support for Terrorism -- Executive Order 13224 Designations E.O. 13224 is an authority aimed at freezing the assets of terrorists and their supporters, and at isolating them from the U.S. financial and commercial systems.”⁴¹

135. The U.S. State Department designated the Qods Force as an FTO in April 2019, along with the IRGC.⁴²

II. HEZBOLLAH, THE QODS FORCE, AND REGULAR IRGC LED A CONSPIRACY TO ACCOMPLISH THEIR “SECURITY” MISSION OF EXPELLING THE UNITED STATES FROM THE MIDDLE EAST AND FULFILL THE IRGC’S CONSTITUTIONAL DUTY TO PROMOTE TERRORISM TO EXPORT THEIR ISLAMIC REVOLUTION

136. Given the complexity of Defendants’ participation in the IRGC Conspiracy as alleged in this Complaint, Plaintiffs first outline the conspiracy’s structure, before proceeding to set forth detailed allegations regarding the same.

⁴¹ *Id.*

⁴² *See* 84 Fed. Reg. 15278-01 (Apr. 15, 2019).

137. In this section, Plaintiffs identify: (A) the object to the conspiracy; (B) the parties to the Conspiracy; (C) how the attacks that occurred in this case were acts in furtherance of the Conspiracy; and (D) the dates on which we think each Defendant joined the Conspiracy and the manner by which they joined the Conspiracy.

A. The Object Of The Conspiracy And Its Leadership

138. The IRGC established the IRGC Conspiracy after 9/11 and it continued, with respect to Afghanistan, until the end of the terrorist campaign in Afghanistan. Today, the IRGC Conspiracy continues wherever Americans are present in the Middle East, including, but not limited to, Iraq, Yemen, Syria, and elsewhere, and the IRGC continues to sponsor attacks against Americans in such countries in furtherance of the Conspiracy.

139. The Object of the IRGC Conspiracy was for the IRGC Shareholders to accomplish their “security” mission of expelling the United States from the Middle East, including Afghanistan and Iraq.

140. The “IRGC Shareholders” who organized the Conspiracy comprised the three constituent parts of the IRGC, i.e., the IRGC’s Hezbollah Division, the IRGC’s Qods Force, and the Regular IRGC (hereinafter, the “IRGC Shareholders”).⁴³

141. On information and belief, at all relevant times, each of the three IRGC Shareholders made a roughly co-equal contribution to the Conspiracy with respect to funds, equipment, weapons, terrorist personnel, technologies, and logistics.

142. **The IRGC’s Hezbollah Division**, has the same meaning as Lebanese Hezbollah, and was one of the leaders of the Conspiracy (hereinafter, “Hezbollah Division” or “Hezbollah”).

⁴³ The IRGC Shareholders are one and the same with the Iranian Shareholders, defined above, because the Iranian Shareholders were merely fronts for the IRGC Shareholders.

- (i) **Role:** Hezbollah was a designated FTO based upon its service as the IRGC's External Security Organization, meaning, Hezbollah's service as the IRGC's lead agent for conducting "External Security" operations (i.e., anti-American terrorism) worldwide. Hezbollah served as the IRGC's "security" proxy specialist worldwide and, as such, was tasked with organizing anti-American "resistance" attack campaigns in, among other places, Afghanistan and Iraq. Hezbollah did all of this to aid the Afghanistan Terror Campaign and Iraq Terror Campaign in furtherance of the Conspiracy.
- (ii) **Leadership:** Hezbollah was commanded by **Hassan Nasrallah** ("Nasrallah"), who was internationally notorious (as covered by the media) around the world for being a terrorist, known within Iran for being a terrorist, and, on information and belief, understood by each Defendant to be an IRGC terrorist operative who served as the head of the Hezbollah Division and commanded some of the largest and most important IRGC terrorist finance, logistics, communications, weapons, narcotics, and operations fronts. Nasrallah did all of this to aid the Afghanistan Terror Campaign and Iraq Terror Campaign in furtherance of the Conspiracy.

143. **The IRGC's Qods Force**, meaning the IRGC's Iranian-staffed external "Security" Operations Division, which at all relevant times worked in close partnership with the IRGC's Hezbollah Division.

- (i) **Role:** The Qods Force was a designated SDGT based upon its service as the IRGC's Iranian-located terror organization that is the flip side of the coin of Hezbollah's External Security Organization and designed to work with Hezbollah through the IRGC's joint cell approach. The Qods Force served alongside Hezbollah as the IRGC's "security" proxy specialist worldwide and, as such, was tasked, alongside Hezbollah, with organizing anti-American "resistance" attack campaigns in, among other places, Afghanistan and Iraq. The Qods Force did all of this to aid the Afghanistan Terror Campaign and Iraq Terror Campaign in furtherance of the Conspiracy.
- (ii) **Leadership:** Until his death in 2020, the Qods Force was commanded by **Brigadier General Qassem Soleimani** ("Soleimani"), who was internationally notorious (as covered by the media) around the world for being a terrorist, known within Iran for being a terrorist, and, on information and belief, understood by each Defendant to be an IRGC terrorist operative who served as the head of the Qods Force and commanded some of the largest and most important IRGC terrorist finance, logistics, communications, weapons, narcotics, and operations fronts, and worked closely with Hezbollah pursuant to the IRGC's joint cell model. Soleimani did all of this to aid the Afghanistan Terror Campaign and Iraq Terror Campaign in furtherance of the Conspiracy.

144. **Regular IRGC**, meaning the IRGC's Internal Security Division (hereinafter as an organization, "Regular IRGC," and as individual members, "IRGC Regulars").

- (i) **Role:** Regular IRGC and the IRGC Regulars who served within it operated *exclusively* within the geographic borders of Iran and served primarily as fronts for IRGC's terrorist finance, logistics, illicit technology acquisition, and intelligence activities, to coordinate the logistics and supply chain needs for the IRGC's Hezbollah Division and Qods Force, through Regular IRGC's fronts and cover companies, charities, and foundations inside Iran, including, but not limited to, the Bonyad Mostazafan, IEI, IEDC, and TCI. Regular IRGC did all of this to aid the Afghanistan Terror Campaign and Iraq Terror Campaign in furtherance of the Conspiracy.
- (ii) **Leadership:** Regular IRGC was commanded by the IRGC terrorist, **IRGC Chief of Staff Mohammad Forouzandeh** ("Forouzandeh"), who internationally notorious (as covered by the media) around the world for being a terrorist, known within Iran for being a terrorist, and, on information and belief, understood by each Defendant to be an IRGC terrorist operative who served as the IRGC Chief of Staff and commanded the largest and most important IRGC terrorist finance, logistics, and operations front, the Bonyad Mostazafan.⁴⁴ Forouzandeh did all of this to aid the Afghanistan Terror Campaign and Iraq Terror Campaign in furtherance of the Conspiracy.

145. To accomplish the object of the Conspiracy by recruiting additional terrorist groups, corporate partners, criminal organizations, and individuals to aid their campaign terrorizing Americans through a coordinated global campaign of terrorist violence facilitated by the IRGC Shareholders in order to conduct "resistance" operations, i.e., anti-American terrorist attacks, in furtherance of the Conspiracy (such joining person, a "Member" of the Conspiracy), each person who joined the Conspiracy organized by the IRGC Shareholders to regularly provide valuable "**Security Aid**" (as Plaintiffs define below) provided such aid, which flowed through the Members to facilitate attacks that aided the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy. Each Member's actions were to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

⁴⁴ Forouzandeh effectively midwived the Qods Force. He was appointed to be chief of staff of the IRGC in order to reorganize it to suit Khomeini's needs. A few years into his tenure, also at Khomeini's direction, Forouzandeh oversaw the creation of the Qods Force, which was formally created in 1990 (his appointment as Chief of Staff, depending on the source, was either in 1986 or 1988).

146. Each Member who joined the Conspiracy had to pledge that they would provide significant aid to help the Iranian Shareholders support their “security” operations, by directly or indirectly facilitating one or more of the following flows of material support to travel from to the Defendants and/or the United States as a result of the Defendant’s conduct, to flow through the Defendant or another entity whom the Defendant owns or otherwise controls, before reaching the persons who committed the attacks that killed and injured Plaintiffs.

147. Each Member facilitated the provision of one or more of the following forms of “Security Aid” to the IRGC (inclusive of each of its IRGC Shareholders) and the Haqqani Network (an FTO and Member of the Conspiracy):

- (i) fundraising to finance terrorist operations, including “tax” collection and diaspora donations);
- (ii) terrorist logistics;
- (iii) attack planning;
- (iv) assassinations and bombings (design and execution);
- (v) illicit technology acquisition;
- (vi) Big Data analytics and management;
- (vii) operations;
- (viii) communications;
- (ix) transportation;
- (x) narcotics trafficking;
- (xi) smuggling; and
- (xii) intelligence operations (each, a form of “**Security Aid**”).

148. Each form of Security Aid materially assisted the Members’ ability to commit attacks to aid the Afghanistan Terror Campaign in furtherance of the Conspiracy.

B. The Parties To The Conspiracy: When Each Member Provided Security Aid To Other Members Of The Conspiracy, Such Member Did So To Aid The Iraq Terror Campaign And Afghanistan Terror Campaign in furtherance of the Conspiracy.

1. FTO/SDGT Co-Conspirators

149. Hezbollah, the Qods Force, and Regular IRGC started the Conspiracy and led it throughout.

150. As to one or more Plaintiffs,⁴⁵ the FTO Co-Conspirators include Hezbollah, al-Qaeda, and the Haqqani Network. (The Taliban, of which the Haqqani Network is a part, is an SDGT.) Each FTO/SDGT Co-Conspirator's actions were to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

151. The Taliban, including its Haqqani Network, joined the Conspiracy at the same time and agreed to facilitate attacks to aid the Iraq Terror Campaign on or about 2005, and the Afghanistan Terror Campaign on or about 2006.⁴⁶

2. Corporate Front Co-Conspirators

152. The corporate fronts or "covers" for the IRGC, who joined the Conspiracy were: (1) MTN Irancell; (2) TCI and MCI; and (3) Exit40. Discovery will likely reveal additional Corporate Front Co-Conspirators.

⁴⁵ Given the IRGC's FTO designation, the FTO status differs per Plaintiff, but the conclusion does not. The FTOs common to all Plaintiffs (i.e., accounting for the IRGC pre- and post-designation) are: Hezbollah and al-Qaeda.

⁴⁶ For the avoidance of all doubt, Plaintiffs do not mean to suggest that these groups were not engaged in terrorist attacks prior to these dates, only that this was when these groups reached agreement with the Iranian Shareholders.

i. MTN Irancell

153. MTN Group Limited (“MTN Group,” together with its subsidiaries, “MTN”) is a South African telecommunications company whose stock trades publicly on the Johannesburg Stock Exchange under the ticker symbol MTN:SJ. Its principal place of business is in Roodepoort, South Africa.

154. MTN Irancell is a joint venture between MTN Group, which has a 49% stake and is not in charge, and the Bonyad Mostazafan and Iran Electronics Industries (“IEI”), which collectively own a 51% stake and are fronts for Hezbollah, the Qods Force, and Regular IRGC. MTN Irancell is an Iranian company and its principal place of business is in Tehran, Iran. MTN Irancell operates as, and MTN Irancell’s employees and agents work as operatives for, a front for Hezbollah, the Qods Force, and Regular IRGC.

155. MTN Irancell was a front for Hezbollah, the Qods Force, and the Regular IRGC.

156. MTN Irancell joined the Conspiracy on or about 2005, when MTN Group’s President and CEO executed the Letter Agreement at in Tehran in the presence of one or more notorious IRGC terrorists, in which MTN Group promised to ensure that MTN Irancell aided the “security” agenda of the “Iranian Shareholders.” Irancell, TCI, and MCI were also co-conspirators.

157. MTN Irancell remains in the Conspiracy today.

158. MTN Irancell served (and continues to serve) as an IRGC front to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

ii. MTN Group

159. MTN Group was a cover for Hezbollah, the Qods Force, and the Regular IRGC.

160. MTN Group joined the Conspiracy on or about 2005, when MTN Group’s President and CEO agreed that MTN Group would cause all of MTN’s subsidiaries and affiliates

to serves as fronts for the “Iranian Shareholders,” which MTN Group’ CEO knew was a direct reference to Hezbollah (an FTO) and the Qods Force.

161. MTN Group’s serial deceptions about the Letter Agreement demonstrate MTN’s consciousness of guilt at having joined the Conspiracy.

162. Thereafter, MTN Group served as a front for the financial and procurement activities of Hezbollah (through Exit40) and all three IRGC Shareholders through their other “Security Aid” identified in the Complaint.

163. MTN Group served as an IRGC cover to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

164. MTN Group authorized the payment of, at a minimum, millions of dollars each year from 2009 through 2020 that MTN Group caused to be paid to the Haqqani Network, which, on information and belief, MTN Group continued to pay even after it was designated an FTO. Each such payment or authorization by MTN Group was an act in furtherance of the Conspiracy because MTN Group knew it was paying money to an ally of the IRGC Shareholders who would use it to aid their proxy terror attacks against Americans in the Middle East. When MTN Group made or authorized each such payment, MTN Group did so to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

165. MTN Group’s promises to pay (in 2005) and payments (in 2007) of a \$400,000 bribe to “Short John” (an IRGC cut-out) and \$200,000 bribe to “Long John” (to corruptly swing a U.N. vote), were acts in furtherance of the Conspiracy because MTN Group knew it was paying money to an ally of the IRGC Shareholders who would use it to aid their proxy terror attacks against Americans in the Middle East. When MTN Group made or authorized each such

payment, MTN Group did so to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

166. MTN Group's attempts to repatriate, and repatriation of, money from Irancell using the mails and wires of the United States from 2012 through 2018 were acts in furtherance of the Conspiracy because, on information and belief, MTN Group had to also authorize a substantial financial transfer to MTN Irancell as a condition of accessing the money, MTN Group knew that this would result in MTN Group causing money to flow to an ally of the IRGC Shareholders who would use it to aid their proxy terror attacks against Americans in the Middle East. When MTN Group made or authorized each such payment, MTN Group did so to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

iii. TCI and MCI

167. TCI and MCI were fronts for Hezbollah, the Qods Force, and the Regular IRGC.

168. TCI and MCI joined the Conspiracy on or about 2009.

169. TCI and MCI remain in the Conspiracy today.

170. TCI and MCI served as an IRGC front to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

iv. Exit40

171. On information and belief, Exit40 ("Exit40") is a front company owned, controlled, and operated by Hezbollah.

172. On information and belief, Exit40 was purpose-built by Hezbollah, following IRGC terrorist tradecraft, to serve as a front for illicit fundraising and acquisition of embargoed U.S. technologies including American smartphones and servers.

173. On information and belief, Exit40 supplied the described Security Aid to other Members of the Conspiracy in order to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

174. On information and belief, Exit40 joined the conspiracy no later than on or about 2005, when MTN Group caused Exit40 to be hired as a consultant or a distributor on behalf of MTN Group, MTN Irancell, or another MTN subsidiary.

175. On information and belief, Exit40 routed tens of millions in value through MTN Group, MTN Dubai, MTN Irancell or another MTN entity, which was all done at the direction of MTN Group, and which flowed the value to Hezbollah from 2005 until on or about 2012. Hezbollah, in turn, shared such resources to facilitate attacks to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

3. Corporate Supplier and Manufacturer Co-Conspirators

176. The IRGC Conspiracy operated through its terrorist members to carry out attacks on Americans, with the IRGC providing logistical and financial support. The attacks in this case were all acts in furtherance of the IRGC Conspiracy. Every person that agreed to join the IRGC Conspiracy is therefore liable for the harm caused by these attacks.

177. Defendant ZTE Corp. and Defendant Huawei Co., like co-conspirator MTN Group, joined the IRGC Conspiracy when they agreed with known IRGC fronts (variously including, but not limited to, MTN Irancell, TCI, MCI, and Exit40) to provide resources, technical materials, and technical support, and to support Iran's "security" objective.

178. ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN Group) agreed to provide such assistance in order to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the IRGC Conspiracy.

179. Each of ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN Group), and each of their U.S. manufacturer co-Defendants, acted in furtherance of that agreement to join the IRGC Conspiracy each time they provided money and other resources, provided technical goods, such as cell phones and telecom infrastructure, assisted with technical support, as was their obligation as joint venturers with and contractual counterparties to known IRGC fronts, when they evaded U.S. sanctions in order to do so, and when they attempted to obfuscate their respective roles.

180. Each time ZTE and Huawei (alongside co-conspirator MTN) did these acts in furtherance of the IRGC Conspiracy, each Defendant assisted the IRGC Conspiracy's objective to attack Americans and furthered the IRGC Conspiracy's ultimate objective to expel Americans from Afghanistan and Iraq.

181. From at least 2005 through 2021, terrorists from Hezbollah, the Qods Force, and Regular IRGC, aided al-Qaeda and the Taliban as the Taliban conspired with Mullah Omar, Sirajuddin Haqqani, and others to conduct and maintain the Taliban as a terrorist enterprise capable of: (1) carrying out sophisticated attacks on American targets in Afghanistan; and (2) aiding the Taliban's co-conspirators, the IRGC (including Hezbollah and the Qods Force) fund attacks on Americans in Iraq and elsewhere in the Middle East through the Taliban, including its Haqqani Network's, assistance to Hezbollah, the Qods Force, and Regular IRGC, to profit from shared narcotrafficking, money laundering, and arms supply activities, all of which were illegal. Throughout that time, the IRGC, inclusive of its Hezbollah Division and Qods Force, al-Qaeda, and the Taliban, inclusive of its Haqqani Network, was a group of associated individuals that functioned as a continuing unit, and the IRGC's, including Hezbollah's and the Qods Force's, al-Qaeda's, and the Taliban's, including the Haqqani Network's express purpose at all times

included the sustainment and propagation of violence against, and the expulsion of, Americans in Afghanistan and Iraq by one or more of the following members of the conspiracy: (i) Hezbollah, the Qods Force, and Regular IRGC, and the Iranian Shareholders who own or control the fronts and/or covers associated with Hezbollah, the Qods Force, and Regular IRGC; (ii) MTN Irancell; (3) Telecommunications Company of Iran; (4) Exit40; (5) al-Qaeda; (6) the Taliban, including its Haqqani Network; (7) Ansar al-Isam; and (8) al-Qaeda-in-Iraq. The Taliban engaged in, and its activities affected, foreign commerce.

C. Plaintiffs Were Injured By Attacks In Afghanistan That Occurred In Furtherance Of The Conspiracy

182. Plaintiffs were injured by attacks that were conducted in one of terrorist campaigns that the IRGC facilitated in furtherance of the IRGC Conspiracy in Afghanistan.

183. Attacks committed in the Afghanistan Terror Campaign strengthened the potency of the Iraq Terror Campaign, and vice versa, because they reduced morale, increased resource strain, promoted efficiencies for the terrorists, provided real-time portable training in the form of live-fire exercises, and promoted the cross-pollination of IRGC Shiite Terrorist Proxies with IRGC Syndicate Terrorist Proxies.

184. Institutional sources of illicit transnational terrorist finance in the Afghanistan Terror Campaign – especially narcotics trafficking – strengthened the potency of the Iraq Terror Campaign, and vice versa, because the Hezbollah and the Qods Force worked closely with al-Qaeda and the Taliban (including its Haqqani Network) to maximize the huge income for all involved. Such strategies produced tens of millions in cross-pollinated income streams between IRGC Shiite Terrorist Proxies with IRGC Syndicate Terrorist Proxies, which increased the flow of resources to facilitate attacks to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

1. The Iraq Terror Campaign

185. The Iraq Terror Campaign comprised terrorist attacks in Iraq from 2006 through 2021 that were committed by IRGC Shiite Terrorist Proxies and/or IRGC Syndicate Terrorist Proxies against Americans in Iraq for the specific purpose of inflicting pain on the United States to drive the United States out of Afghanistan and Iraq in furtherance of the IRGC Conspiracy, where the FTO or FTOs that committed the attack received material support from Hezbollah, the Qods Force, and Regular IRGC to aid such attacks against Americans in Iraq.

2. The Afghanistan Terror Campaign

186. The Afghanistan Terror Campaign comprised terrorist attacks in Afghanistan from 2007 through 2021 that were committed by IRGC Shiite Terrorist Proxies and/or IRGC Syndicate Terrorist Proxies against Americans in Afghanistan for the specific purpose of inflicting pain on the United States to drive the United States out of Afghanistan and Iraq in furtherance of the Conspiracy, where the FTO or FTOs that committed the attack received material support from Hezbollah, the Qods Force, and Regular IRGC to aid such attacks against Americans in Afghanistan.

187. The Afghanistan Terror Campaign unfolded much in the same manner as the Iraq Terror Campaign but started about a year later (the IRGC began with Iraq before broadening to Afghanistan).

188. In 2005, Hezbollah, the Qods Force, and the Regular IRGC helped kickstart the Afghanistan Terror Campaign. Hezbollah, the Qods Force, and the Regular IRGC did so to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the Conspiracy.

189. On or about 2006, the Taliban, including its Haqqani Network, joined the Conspiracy. On information and belief, the Taliban, including its Haqqani Network did so after

a series of meetings between emissaries in Afghanistan and Iran, including, but not limited to, in Herat, Afghanistan, and Mashhad, Iran.

190. Attacks committed in the Afghanistan Terror Campaign strengthened the potency of the Iraq Terror Campaign, and vice versa, because they reduced morale, increased resource strain, promoted efficiencies for the terrorists, provided real-time portable training in the form of live-fire exercises, and promoted the cross-pollination of IRGC Shiite Terrorist Proxies with IRGC Syndicate Terrorist Proxies.

191. Institutional sources of illicit transnational terrorist finance in the Afghanistan Terror Campaign – especially narcotics trafficking – strengthened the potency of the Iraq Terror Campaign, and vice versa, because the Hezbollah and the Qods Force worked closely with al-Qaeda and the Taliban (including its Haqqani Network) to maximize the huge income for all involved. Such strategies produced tens of millions in cross-pollinated income streams between IRGC Shiite Terrorist Proxies with IRGC Syndicate Terrorist Proxies, which increased the flow of resources to facilitate attacks to aid the Iraq Terror Campaign and Afghanistan Terror Campaign in furtherance of the IRGC Conspiracy.

192. Each Afghanistan Plaintiff was injured in an attack committed by one or more of the above-identified designated FTOs who joined the IRGC Conspiracy and committed the attack in furtherance of the Conspiracy.

III. AFTER 9/11, HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, TALIBAN, AND AL-QAEDA JOINED A CONSPIRACY LED BY THE IRGC TO DRIVE THE UNITED STATES OUT OF AFGHANISTAN, IRAQ, AND THE MIDDLE EAST THROUGH ATTACKS SUPPORTED BY COMMON FUNDING SOURCES, TECHNOLOGIES, AND CORPORATE PARTNERS IN ORDER TO SUSTAIN A TERRORIST ALLIANCE THAT COULD COUNTER NATO

A. The Formation Of The Conspiracy

1. After 9/11, Hezbollah, The Qods Force, And Regular IRGC Led A Terrorist Conspiracy Targeting Americans In Afghanistan, Iraq, And Elsewhere To Inflict Pain On “The Great Satan”

193. After 9/11, the IRGC organized a transnational terrorist alliance – the Islamists’ answer to NATO – in order to marshal efficiencies across the anti-American terrorists, thereby maximizing the lethality of their shared terrorist campaign.

194. By 2007, under the leadership of Qassem Soleimani, Hezbollah and the Qods Force had organized “resistance” (i.e., terror) cells in dozens of countries on six continents. As the *Montreal Gazette* reported at the time:

Under the Ahmadinejad administration, U.S. officials said, the [IRGC] has moved increasingly into commercial operations, *earning profits* and extending its influence in Iran in areas involving big government contracts, including ... *providing cell phones*. Washington has claimed the Revolutionary Guard’s Quds Force wing is responsible for the growing flow of explosives, roadside bombs, rockets and other arms to Shiite militias in Iraq and the Taliban in Afghanistan. Quds Force has also been blamed for supporting Shiite allies such as Lebanon’s Hezbollah and to such Sunni movements as s...⁴⁷

2. To Maximize The Lethality Of Their Terrorist Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Provided Material Support To Every Other Member of the Conspiracy, Including Funds, Arms, Training, And Logistical Support, Which Their Co-Conspirators Used To Attack Americans in Afghanistan

195. After 9/11, Hezbollah, the Qods Force, and Regular IRGC, organized a global terrorist alliance comprised of a litany of allied Shiite and Sunni terrorist groups. Generally,

⁴⁷ Montreal Gazette (Canada), *What is the Revolutionary Guard?* (Aug. 16, 2007), 2007 WLNR 28659733.

such groups could be divided between, on the one hand, transnational groups which seek to attack Americans anywhere, or regional groups, which focus on a geography.

196. In all cases, however, the terrorists: (a) sought to attack and kill Americans to force the United States to withdraw from the Middle East, including Afghanistan and Iraq; and (b) relied upon a network of terrorist allies – an Islamist NATO – necessary to counteract the U.S.-led coalitions in Afghanistan and Iraq, which organized the world’s most powerful militaries and intelligence services to confront these terrorists.

197. Simply put, the IRGC and its terrorist co-conspirators knew they needed their own transnational alliance with all the same functionalities as NATO to successfully prosecute a global terror campaign against Americans on multiple continents for decades.

198. After 9/11, the IRGC’s Hezbollah Division and Qods Force led the IRGC’s support for this conspiracy. With respect to the Hezbollah Division, Hezbollah’s terrorist mastermind, Imad Mugniyeh, led this effort until the U.S. and Israel killed him in 2008, after which Mugniyeh was replaced by other well-trained and experienced Hezbollah Division terrorist operatives. With respect to the Qods Force, the IRGC’s terrorist mastermind, Qassem Soleimani, led the Qods Force-related aspects of the scheme until his own death at the hands of a U.S. drone strike in 2020.

199. To operationalize the various nodes of the conspiracy – including transnational logistics, financial relationships, arms pipelines, smuggling routes, and the like – Hezbollah and the IRGC worked hand-in-hand with each other globally (as they have since the IRGC “midwived” Hezbollah to execute this conspiracy). Hezbollah and the Qods Force followed the same terrorist playbook and tradecraft around the world, which essentially breaks down into two modes of support.

i. IRGC Shiite Terrorist Proxies

200. If Hezbollah and the Qods Force were (a) sectarian allies with the proxy terrorists, meaning that everyone is Shiite, e.g., Hezbollah, the Qods Force, and Jaysh al-Mahdi; or (b) had a long-standing alliance regardless of sect, e.g., their 30+ years of supporting the Sunni terrorist groups Hamas and Palestinian Islamic Jihad, then (c) the IRGC's doctrine mandated that Hezbollah and the Qods Force follow the joint cell model.

201. In such a case, the groups established joint cells comprised of Hezbollah, Qods Force, and their local terrorist proxy to attack Americans in the country in question, or to provide logistical, weapons, operational, financial, or concealment support to another part of the conspiracy that targeted Americans outside of their own country, e.g., a joint cell comprised of Hezbollah, the Qods Force, and allied Syrian operatives who manage a listening post on the Syrian side of the Iraqi border designed to facilitate logistics flow benefiting the terrorist campaign in Iraq and the broader Middle East. The IRGC terrorist proxies who joined the conspiracy under this approach include, but are not limited to:

- (i) **Jaysh al-Mahdi**, which Hezbollah, the Qods Force, and Regular IRGC, supported through their global network of cells with respect to their logistics, funding, transportation, arms supply, and which Hezbollah and the Qods Force supported inside of Iraq through the participation of Hezbollah and Qods Force operatives in joint cells in Iraq comprised of Hezbollah, Qods Force, and Jaysh al-Mahdi terrorist working together as an integrated unit;
- (ii) **the Houthis**, which Hezbollah, the Qods Force, and Regular IRGC, supported through their global network of cells with respect to their logistics, funding, transportation, arms supply, and which Hezbollah and the Qods Force supported inside of Yemen through the participation of Hezbollah and Qods Force operatives in joint cells in Yemen comprised of Hezbollah, Qods Force, and Houthi terrorist working together as an integrated unit;
- (iii) **Hamas and Palestinian Islamic Jihad**, which Hezbollah, the Qods Force, and Regular IRGC, supported through their global network of cells with respect to their logistics, funding, transportation, arms supply, and which Hezbollah and the Qods Force supported inside of Israel through the participation of Hezbollah and Qods Force operatives in joint cells comprised of Hezbollah, Qods Force, and Hamas and/or Palestinian Islamic Jihad terrorist working together as an integrated unit; and the

- (iv) **Assad Regime “Security” Forces**, which Hezbollah, the Qods Force, and Regular IRGC, supported through their global network of cells with respect to their logistics, funding, transportation, arms supply, and which Hezbollah and the Qods Force supported inside of Syria through the participation of Hezbollah and Qods Force operatives in joint cells in Syria comprised of Hezbollah, Qods Force, and Assad regime “security” operatives working together as an integrated unit (collectively, **“IRGC Shiite Terrorist Proxies”**).⁴⁸

202. Hezbollah, the Qods Force, and Regular IRGC, relied upon the full complement of its global terrorist finance, arms, logistics, personnel, communications, operations, and training infrastructure to fund, arm, equip, train, transport, protect, and facilitate terrorist attacks by IRGC Shiite Terrorist Proxies against Americans in Iraq, Syria, Yemen, Lebanon, the United Arab Emirates, Iran, and Afghanistan.

203. Hezbollah, the Qods Force, and Regular IRGC, materially aided every aspect of the IRGC Shiite Terrorist Proxies’ terrorist campaigns against Americans in Iraq, Afghanistan, Yemen, Syria, Lebanon, Europe in furtherance of the conspiracy.

204. Hezbollah, the Qods Force, and Regular IRGC, materially aided every aspect of the IRGC Shiite Terrorist Proxies’ terrorist campaign against Americans in Iraq in furtherance of the IRGC’s conspiracy.

205. To facilitate terrorist attacks against Americans by IRGC Shiite Terrorist Proxies, Hezbollah, the Qods Force, and Regular IRGC, depended upon the large flow of money, equipment, weapons, and logistical support, as well as the “cover” provided by the corporate entity, from the complicit corporate partners, including MTN Irancell, TCI, and any corporate allies that conspired with the IRGC to create and operate these terrorist fronts.

⁴⁸ Please note that this category also includes certain non-Shiite groups that have decades-long client relationships with the Hezbollah and the Qods Force, such as Hamas and Palestinian Islamic Jihad. While Sunni, these two groups have become so embedded in the transnational Shiite terror architecture that they fit within this category, notwithstanding their sectarian affiliation.

ii. IRGC Syndicate Terrorist Proxies

206. If Hezbollah and the Qods Force did *not* have a decades-long alliance with the terrorist proxy and were also not sectarian allies, then the IRGC and Hezbollah followed a different approach, which was the terrorist equivalent to President Ronald Reagan’s famous maxim: “trust but verify.” Under this approach, Hezbollah and the Qods Force, backed by all the money and logistics the IRGC could provide, identified Sunni terrorist groups that could serve as allies of convenience for their shared terrorist agenda against the United States. The IRGC terrorist proxies who joined the conspiracy under this approach include, but are not limited to:

- (i) **al-Qaeda**, which Hezbollah and the Qods Force supported through their global network of cells with respect to their logistics, funding, transportation, arms supply, and which Hezbollah and the Qods Force supported inside of Iran, Iraq, Afghanistan, and Pakistan, through the provision of funds, safe haven, communications, and logistical support; and
- (ii) **the Taliban and its Haqqani Network**, which Hezbollah and the Qods Force supported through their global network of cells with respect to their logistics, funding, transportation, arms supply, and which Hezbollah and the Qods Force supported inside of Iran, Iraq, Afghanistan, and Pakistan, through the provision of funds, arms, training, safe haven, communications, and logistical support⁴⁹ (al-Qaeda and the Taliban, collectively, “**IRGC Syndicate Terrorist Proxies**”).

207. Hezbollah, the Qods Force, and Regular IRGC, materially aided every aspect of the IRGC Syndicate Terrorist Proxies’ terrorist campaigns against Americans in Afghanistan, Iraq, Yemen, Syria, Lebanon, Europe in furtherance of the conspiracy.

⁴⁹ Hezbollah, the Qods Force, al-Qaeda, and the Taliban, including its Haqqani Network, sometimes combined forces to jointly commit an attack against Americans in Afghanistan, Iraq, or another geography to which every organization could contribute or network connections. On information and belief, all these groups coordinated – in a plot led by Brigadier General Esmail Ghaani of the Qods Force and Sirajuddin Haqqani of al-Qaeda and the Taliban, including its Haqqani Network – to facilitate one or more joint Qods Force/Haqqani Network attacks in Afghanistan in 2020 and/or 2021 as explicit retaliation for the January 2020 U.S. drone strike in Iraq that killed Qassem Soleimani (head of Qods Force) and Abu Muhandis (head of Jaysh al-Mahdi Special Group Kataib Hezbollah).

208. To facilitate terrorist attacks against Americans by IRGC Syndicate Terrorist Proxies, Hezbollah, the Qods Force, and Regular IRGC, depended upon the large flow of money, equipment, weapons, and logistical support, as well as the “cover” provided by the corporate entity, from the complicit corporate partners, including MTN Irancell, TCI, and any corporate allies that conspired with the IRGC to create and operate these terrorist fronts.

B. In Furtherance Of The Conspiracy, Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, The Taliban, Including Its Haqqani Network, And The Members Of The Al-Qaeda-Taliban Terrorist Syndicate Waged A Deadly Terrorist Campaign Against Americans In Afghanistan

209. The IRGC’s support of terrorist proxies like Hezbollah, Hamas, the Taliban, and al-Qaeda is well-documented.⁵⁰ The IRGC has also long provided material support to al-Qaeda and the Taliban. In both instances, the sectarian differences between the Shiite regime in Tehran and the Sunni al-Qaeda/Taliban leadership have not hindered cooperation between the groups. Whatever their religious differences, both groups share a hatred of America and support anti-American violence.

210. While Americans worked to rebuild post-war Afghanistan, they were attacked by Taliban and al-Qaeda terrorists. Hezbollah, the Qods Force, and Regular IRGC, sponsored those terrorist attacks in an effort to undermine American foreign policy in Afghanistan. To that end, Hezbollah, the Qods Force, and Regular IRGC, supported the Taliban, including its most radical part, the Haqqani Network, by, among other things, training Taliban terrorists how to attack Americans effectively and paying terrorists who killed U.S. forces. Hezbollah, the Qods Force, and Regular IRGC also provided the Taliban with sophisticated weapons that it used to kill and injure thousands of Americans.

⁵⁰ See Alireza Nader, Joya Laha, *Iran’s Balancing Act in Afghanistan* at 9 (RAND Corp. 2011) (“*Iran’s Balancing Act*”).

211. The IRGC's, including Hezbollah's and the Qods Force's, support for al-Qaeda was equally potent. That support dates back decades and has included money, weapons, training, logistical assistance, and safe harbor for key al-Qaeda leaders. In 2007, Osama bin Laden himself referred to Iran as al-Qaeda's "main artery for funds, personnel, and communication." The IRGC's, including Hezbollah's and the Qods Force's, longstanding decision to back al-Qaeda despite sectarian differences between the two reflected Iran's overriding desire to foment anti-American terrorism around the world. That decision, like the one to provide material support to the Taliban, paid dividends. The IRGC's, including Hezbollah's and the Qods Force's, support for al-Qaeda's activities in Afghanistan substantially contributed to the terrorist violence that killed and injured Americans there.

212. The IRGC's, including Hezbollah's and the Qods Force's, support for al-Qaeda complemented its support for the Taliban because of the close relationship between the two terrorist groups. Although al-Qaeda and the Taliban were nominally separate groups, they acted together in a terrorist "syndicate" that planned and authorized terrorist violence throughout Afghanistan. That syndicate – which involved mafia-style meetings between leaders of the syndicate's various members – provided a superstructure that organized and facilitated a range of terrorist attacks in Afghanistan. By funneling material support to multiple members of that syndicate, Hezbollah, the Qods Force, and Regular IRGC, ensured that the IRGC's policy of sponsoring anti-American terrorism in Afghanistan achieved maximum effect.

213. After 9/11, Hezbollah and the Qods Force operationalized a sophisticated pipeline for routing material support to al-Qaeda and the Taliban to facilitate attacks against Americans in Afghanistan through which the IRGC supplied al-Qaeda and the Taliban with the communications technologies, including cell phones, they needed and trained them how to use

them as terrorist weapons. Indeed, in 2012, the U.K. government publicly accused the IRGC of transferring mobile phones to Taliban terrorists targeting Coalition forces in Afghanistan, and also accused the IRGC of training Taliban terrorists concerning how to deploy such IRGC-provided mobile phones in order to improve the lethality and effectiveness of the Conspiracy's IED attacks targeting Americans in Afghanistan:

- (i) "Iranian bomb makers are suspected of being behind the device which killed the six soldiers." ... "Funded partly by the Taliban, the [Iranian] instructors have taught insurgents in Helmand to disguise bombs from electronic detection, producing a bigger and more deadly blast."
- (ii) "Intelligence experts believe Iran is increasingly influencing the style and impact of attacks against ... [NATO] troops in southern Afghanistan." ... "According to military sources, at least two Iranian active service units have operated in Helmand ... the Iranians ... are suspected of teaching the bomb makers involved the techniques needed to avoid roadside counter-measures."
- (iii) "Border officials in Herat, a city on Afghanistan's western border with Iran, have reported that a wide range of material made in Iran—including mortars, plastic explosives, propaganda materials *and mobile phones*—is also ending up in insurgents' hands. And a Taliban commander admitted that the insurgents had grown more dependent on Iran ..."
- (iv) "[T]he Iranians have taught Taliban fighters to link mobile phones to the bomb, allowing the trigger man to watch for a suitable target before he strikes. ... The Taliban has been using three types of IED: the roadside bomb where an insurgent detonates the device by wire, the remote bomb set off by radio or mobile phone signal and the conventional landmine which is buried beneath the road surface before being detonated by the pressure of a passing vehicle. ... [The Taliban's IED] techniques have become increasingly sophisticated, intelligence officials say, under the influence of the Iranians."⁵¹

214. The IRGC's conspiracy succeeded. The U.S. substantially completed its withdrawal from Afghanistan on or about August 2021, which was one of the four primary objects of the conspiracy. Afghanistan was also, along with Iraq, one of the two central theaters

⁵¹ See, e.g., David Williams, *The Iran Connection: How Taliban Learned To Make Undetectable Bombs*, Daily Mail (Mar. 8, 2012), 2012 WLNR 5017775.

where both Hezbollah, the Qods Force, and Regular IRGC, and the IRGC's Sunni allies al-Qaeda and the Taliban, regularly collaborated in a two-way manner, sharing resources, personnel, smuggling routes, financiers (in-country and around the world), and sometimes even jointly committing attacks with one another.

215. The public reaction of the IRGC, including its Hezbollah Division and Qods Force, to the U.S. withdrawal from Afghanistan confirms that the terrorists believe they achieved one of the objects of the conspiracy:

216. Plaintiffs identify below several terrorist groups, subgroups, and partnerships responsible for the specific attacks that killed and injured them. Each worked in concert and shared resources, personnel, and operational plans. Indeed, the Taliban and al-Qaeda often participated in mafia-style meetings – attended by the leaders of several allied terrorist groups – in which they planned and authorized various terrorist attacks throughout Afghanistan.⁵² Given such coordination, one former CIA official and senior White House advisor called the resulting terrorist superstructure a “syndicate,” composed of al-Qaeda, the Taliban, and several allied FTOs.⁵³ In fact, bin Laden himself conceived of al-Qaeda as the leader of a broader coalition of terrorists drawing from other terrorist organizations in Pakistan and Afghanistan.⁵⁴

217. Iran's support for multiple components of this “syndicate” ensured that its support had maximum effect. Due to the mutually reinforcing ties between the Taliban and al-Qaeda in Afghanistan, support for the one benefited the other – and vice versa. Iran recognized those

⁵² See Bill Roggio and Thomas Joscelyn, *The al Qaeda – Taliban Connection*, Wash. Exam'r (July 4, 2011) (“*The al Qaeda-Taliban Connection*”), archived at <https://www.washingtonexaminer.com/weekly-standard/the-al-qaeda-taliban-connection>.

⁵³ Bruce Riedel, *Deadly Embrace: Pakistan, America, And The Future Of The Global Jihad* at 1 (Brookings Inst. Press 2d ed. 2011).

⁵⁴ *The al Qaeda-Taliban Connection*.

interrelationships and so spread its support across multiple parts of the Afghan terror syndicate. In doing so, Iran was able to achieve its intended effect: wide-ranging terrorist attacks against Americans, executed mostly by the Taliban but supported by (and sometimes jointly committed with) al-Qaeda and the other components of the syndicate.

218. Against that backdrop, Plaintiffs identify below the principal Afghan terrorist groups, subgroups, and cells that committed the attacks that killed and injured them. Plaintiffs also identify how Hezbollah, the Qods Force, and Regular IRGC, facilitated terrorist attacks by al-Qaeda, the Taliban (including its Haqqani Network), and their allies.

1. Al-Qaeda

219. Since its inception, al-Qaeda doctrine has emphasized terrorist strategy that borrows heavily from cooperative game theory principles, including concepts such as cooperation theory, franchising, and joint ventures. “Since the September 11, 2001 terrorist attacks, al Qaeda emerged as the head of a global Islamist terror movement, comprised of dozens of deadly jihadist groups” and “[s]everal members of the al Qaeda terror movement [were] designated as FTOs” including, but not limited to, “Islamic Movement of Uzbekistan,” “Jaish-e-Mohammed,” and “Lashkar-e-Tayyiba.”⁵⁵ This reflected al-Qaeda’s tactical and operational fusion with its affiliates in Afghanistan and Pakistan.

220. Since 9/11, and continuing through the present, Al-Qaeda led the Syndicate and worked jointly with its inseparable ally, the Taliban, with whom al-Qaeda had been essentially fused since before 9/11 and have remained so ever since. The overlap between the organizations meant that al-Qaeda often played a key role in Taliban and Haqqani Network attacks. As

⁵⁵ Jimmy Gurulé, *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* 89 (Edward Elgar 2008) (hereinafter, “Gurulé, *Unfunding Terror*” or “Gurulé”).

terrorism scholars Bill Roggio and Thomas Joscelyn observed, “[i]t is not clear where, say, al Qaeda ends and the Taliban and other terrorist groups begin. This is by design. Bin Laden envisioned al Qaeda as the vanguard of a broader jihadist coalition. Al Qaeda was always a joint venture.”⁵⁶ Mr. Joscelyn testified that the word “syndicate” – referring to al-Qaeda’s terrorist joint venture with its Afghan and Pakistani affiliates – offers an “excellent description of how al Qaeda operates.”⁵⁷

221. The U.S. State Department designated al-Qaeda as a FTO on October 8, 1999.

222. Al-Qaeda’s and the Taliban’s close relationship continued long after 9/11. In the years since, it has become clear that the al-Qaeda and Taliban organizations have been fused together: al-Qaeda terrorists have often worked in close conjunction with Taliban terrorists and the affiliated Haqqani Network and Kabul Attack Network. In May 2007, Taliban official Mullah Dadullah said, “[W]e and al-Qaeda are as one.”⁵⁸ In early 2009, a military-intelligence official was quoted as saying, “The line between the Taliban and al Qaeda is increasingly blurred, especially from a command and control perspective.”⁵⁹ By the end of that year, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen said the same thing openly. “We are deeply concerned about the growing level of collusion between the Taliban and al Qaeda,” he told *The Wall Street Journal*.⁶⁰ And as Lieutenant General Ronald L. Burgess, Jr. reported in a

⁵⁶ *The al Qaeda – Taliban Connection*.

⁵⁷ *Al-Qaeda In Afghanistan and Pakistan: An Enduring Threat*, Hr’g Before the U.S. House Committee On Foreign Affairs, Subcommittee On Terrorism, Nonproliferation, and Trade, S. Hr’g 113-156, at 28 (May 20, 2014) (statement of Thomas Joscelyn, Sr. Research Fellow, Found. for Def. of Democracies), 2014 WLNR 13518260.

⁵⁸ Thomas Ruttig, *The Other Side* 23, Afghanistan Analysts Network (July 2009).

⁵⁹ Bill Roggio, *Al Qaeda Builds A ‘Shadow Army’*, Wash. Times (Feb. 13, 2009).

⁶⁰ Anand Gopal, *Afghan Police Killings Highlight Holes in Security*, Wall St. J. (Dec. 15, 2009).

February 2010 Hearing of the Senate Select Committee on Intelligence, “al Qaeda’s propaganda, attack planning and support of the Taliban and Haqqani networks continues.”⁶¹

223. By 2009, al-Qaeda and the Haqqani Network intensified their attack campaign inside Afghanistan. To do so, they ramped up their terrorist finance campaigns worldwide, putting out a call to all al-Qaeda and Haqqani Network financiers to support the jihad against Americans in Afghanistan the same way both groups had previously rallied terrorist financiers worldwide to support the campaign against the Soviets in the 1980s.

224. Thereafter, due in large part to the Syndicate’s terrorist finance, al-Qaeda’s terrorist campaign grew more lethal each month and year.

225. Al-Qaeda’s Syndicate-counterattack-strategy reflected bin Laden’s long-standing vision of al-Qaeda (and him, specifically) as the leader of a grand terrorist coalition across Afghanistan and Pakistan.⁶² Due to the mutually reinforcing ties between al-Qaeda, the Taliban (including its Haqqani Network), Lashkar-e-Taiba, and D-Company in Afghanistan – including their practice of cross-donations to each other – support for one benefited all. Defendants’ support to the Syndicate’s terrorist finance bombmaking logistics thus had crosscutting effects: they enabled wide-ranging terrorist attacks against Americans in Afghanistan.

226. Al-Qaeda’s leadership of that terrorist syndicate reflected the degree to which al-Qaeda and the Taliban became fully and operationally intertwined. As India’s Permanent Representative to the United Nations explained in describing the al-Qaeda-Taliban “syndicate of

⁶¹ Transcript, Hr’g Of The Senate Select Committee On Intelligence Subject: "Current And Projected Threats To The United States, Fed. News Serv., 2010 WLNR 27828348 (Feb. 2, 2010).

⁶² See Bill Roggio & Thomas Joscelyn, *The al Qaeda – Taliban Connection*, Weekly Standard (July 4, 2011) (“*The al Qaeda – Taliban Connection*”).

terrorism,” both groups were by 2011 “ideologically and operationally fused.”⁶³ By the fall of 2009, noted journalist Peter Bergen concluded, “the Taliban and Al Qaeda function more or less as a single entity. The signs of this are everywhere.”⁶⁴

227. Internationally, al-Qaeda and the Haqqani Network (and through it, the Taliban) shared intertwined streams for fundraising, financing, logistics, smuggling, and weapons. According to Haqqani Network expert Gretchen Peters, international “funding streams” were “intertwined across” amongst al-Qaeda, the Haqqani Network, and the Taliban.⁶⁵ As Ms. Peters explained in 2012, al-Qaeda, the Haqqani Network, and their allies “derive[d] income in and outside Afghanistan” and their “money move[d] between key network actors and into banks in Pakistan, the [U.A.E.] and beyond.”⁶⁶

228. The Taliban and al-Qaeda have remained intimately intertwined. For example, in 2015, Osama bin Laden’s successor, Ayman Zawahiri, pledged an oath of allegiance to the recently-installed Taliban leader Mullah Akhtar Mohammad Mansour, who publicly announced his acceptance of the pledge the following day.⁶⁷ When Mansour was killed in May 2016, Zawahiri pledged allegiance to his successor, Mawlawi Haibatullah Akhundzada.

⁶³ *India Against Hasty Troop Withdrawal From Afghanistan*, Daily Fin. Post (Oct. 1, 2011), 2011 WLNR 20105460 (quoting Hardeep Singh Puri, India’s Permanent Representative to the United Nations).

⁶⁴ Peter Bergen, *The Front: The Taliban-Al Qaeda Merger*, New Republic (Oct. 19, 2009) (“*The Front*”).

⁶⁵ Gretchen Peters, *Haqqani Network Financing: The Evolution Of An Industry* 32, Combatting Terrorism Ctr. (July 2012) (“Peters, *Haqqani Network Financing*”).

⁶⁶ *Id.*

⁶⁷ Thomas Joscelyn & Bill Roggio, *New Taliban Emir Accepts al Qaeda’s Oath Of Allegiance*, Long War J. (Aug. 14, 2015).

229. Often, individual Taliban leaders are also members of al-Qaeda. For example, in late 2011 or early 2012 the Taliban appointed Sheikh Mohammed Aminullah, who has close ties to al-Qaeda, as the head of its Peshawar Regional Military Shura, which is responsible for attacks in northern and eastern Afghanistan.

230. Al-Qaeda also encouraged the Taliban to embrace new terrorist techniques. In February 2003, bin Laden issued a recording calling specifically for suicide attacks in Afghanistan and Iraq. Taliban terrorists had previously viewed suicide attacks as taboo, but al-Qaeda convinced them they were religiously permissible. Indeed, al-Qaeda trumpeted their ideological success online, announcing, “While suicide attacks were not accepted in the Afghani culture in the past, they have now become a regular phenomenon!”⁶⁸ With al-Qaeda’s encouragement and training, the number of such suicide attacks in Afghanistan increased from one in 2002, two in 2003, and six in 2004, to 21 in 2005 and more than 100 in 2006. Al-Qaeda further encouraged these attacks by paying the families of suicide bombers in Afghanistan.

231. Al-Qaeda’s role in that suicide-bombing trend was pivotal. As Islamic history scholar Bryan Glyn Williams explained, “Al Qaeda operatives carried out two to three [suicide] bombings per year on the Afghan government and NATO troops from 2002 to 2004 that were meant to demonstrate the effectiveness of this alien tactic to the local Taliban. These demonstrative acts and videos of successful [Al Qaeda] suicide bombings in Iraq seem to have convinced the Taliban to condone the previously taboo tactic of suicide bombing.”⁶⁹

⁶⁸ Brian Glyn Williams, *Suicide Bombings In Afghanistan*, Jane’s Islamic Affairs Analyst at 5 (Sept. 2007).

⁶⁹ Bryan Glyn Williams, *Afghanistan Declassified: A Guide to America’s Longest War* at 202 (Univ. Penn. Press 2012).

232. Al-Qaeda operatives also served as embedded trainers with Taliban forces. These experienced trainers provided instructions, funding, and resources for conducting local and international attacks. By 2005 at the latest, al-Qaeda began bringing instructors from Iraq to train the Taliban how to fight Americans. For example, al-Qaeda members trained Taliban commanders in bomb-making techniques. Al-Qaeda also invited Taliban commanders to Iraq, where they learned how to make armor-penetrating “shaped” charges,⁷⁰ a type of IED later known as an EFP. Taliban trainees also learned how to use remote controls and timers, and urban warfare tactics.

233. As one writer put it in November 2009, “[s]mall numbers of Al Qaeda instructors embedded with much larger Taliban units have functioned something like U.S. Special Forces do – as trainers and force multipliers.”⁷¹

234. By the mid-2000s, al-Qaeda’s partnership with the Haqqani Network had facilitated the emergence of a network of al-Qaeda training camps in North Waziristan. According to a declassified 2008 Defense Intelligence Agency intelligence report.⁷²

235. Al-Qaeda has also established multiple training camps within Afghanistan reportedly “hosted by the Taliban.”⁷³ One such camp covered nearly 30 square miles and

⁷⁰ Sami Yousafzai, *Unholy Allies*, Newsweek (Sept. 25, 2005).

⁷¹ Peter Bergen, *The Front*, New Republic (Oct. 19, 2009), <https://newrepublic.com/article/70376/the-front>.

⁷² Defense Intelligence Agency, *Location and Activities of the Training Centers Affiliated with the Haqqani Network, Taliban, and al-Qaeda in Northern Waziristan and Future Plans and Activities of Sarajuddin ((Haqqani))*, Intelligence Information Report (Apr. 16, 2008), <https://www.dia.mil/FOIA/FOIA-Electronic-Reading-Room/FOIA-Reading-Room-Other-Available-Records/FileId/155424/>.

⁷³ Thomas Joscelyn and Bill Roggio, *Trump’s Bad Deal With The Taliban*, Politico (Mar. 18, 2019).

contained heavy weapons, IED-making material, anti-aircraft weapons, rocket-propelled grenade systems, machine guns, pistols, rifles, and ammunition.

236. On top of the myriad forms of support detailed above, al-Qaeda also jointly planned and authorized terrorist attacks that the Taliban carried out. Those joint planning sessions often occurred in meetings in which al-Qaeda, the Taliban, and other members of the al-Qaeda-Taliban syndicate (such as Lashkar-e-Taiba) would confer about particular geographies and targets to attack.⁷⁴ The close operational coordination not only manifested itself in the Kabul Attack Network, but also provided a broader terrorist superstructure that organized the insurgency throughout Afghanistan. In observing that this superstructure formed an Afghan-Pakistani “syndicate” of sorts, a former CIA analyst and White House advisor documented several notable syndicate-sponsored terrorist attacks in Afghanistan that “demonstrated the intricate connections between al Qaeda and its allies in Pakistan and Afghanistan.”⁷⁵ Those intimate connections enhanced the lethality of the overall anti-American insurgency.

237. Information derived from al-Qaeda and Taliban detainees held at Guantanamo Bay, Cuba (“Gitmo”) corroborates the planning and authorization activities of the al-Qaeda-Taliban syndicate. For example, according to purported Gitmo intelligence files quoted by terrorism experts Bill Roggio and Thomas Joscelyn, one detainee, Abdul Razak, was a “high-level military commander in a newly-conceived ‘unification’ of Al Qaeda, [Hezb-e-Islami Gulbuddin (“HIG”),] and Taliban forces within Afghanistan,” which the leaders of the respective terrorist groups “envisioned [as a] new coalition of HIG, Al Qaeda, and Taliban during a meeting

⁷⁴ *The al Qaeda-Taliban Connection*.

⁷⁵ Bruce Riedel, *Deadly Embrace: Pakistan, America, And The Future Of The Global Jihad* at 100 (Brookings Inst. Press 2d ed. 2011).

in Pakistan in early spring 2003.”⁷⁶ Another purported Gitmo detainee file quoted by Messrs. Roggio and Joscelyn concerning Haroon al Afghani, a dual-hatted al-Qaeda/HIG terrorist, contained the following intelligence report:

[Afghani] is assessed to have attended a joint operations meeting among extremist elements in mid-2006. A letter describing an 11 August 2006 meeting between commanders of the Taliban, al Qaeda, [Lashkar e Taiba], . . . and the Islamic Party (probably a reference to the HIG), disclosed that the groups decided to increase terrorist operations in the Kapisa, Kunar, Laghman, and Nangarhar provinces, including suicide bombings, mines, and assassinations.⁷⁷

238. Taken together, these reports “demonstrate a high degree of collusion between al Qaeda and other terrorist groups” as part of a “jihadist hydra” that shares the “common goal” of seeking to “drive the U.S.-led coalition out of Afghanistan.”⁷⁸ One al-Qaeda operative, whom U.S. officials characterized as “an important al-Qaida planner and explosives expert,” Ghazwan al-Yemeni, trained Taliban members in Pakistan.⁷⁹ He eventually helped plan the December 30, 2009 attack on Camp Chapman that killed seven Americans.⁸⁰

239. Al-Qaeda doctrine emphasized the development and deployment of dual- or even triple-hatted terrorists, whom counter-terror and counter-narcotics professionals describe as “polyterrorists” (or “poly-traffickers”). Al-Qaeda fashioned itself a multi-national corporation for Islamist terrorists, and therefore embraced an aggressive expansion strategy in the late 1990s, which accelerated even more after 9/11, in which al-Qaeda scaled up by making new partners from other terrorist groups.

⁷⁶ *The al Qaeda – Taliban Connection*.

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ Evan F. Kohlmann, *Al-Qa’ida’s Yemeni Expatriate Faction in Pakistan*, CTC Sentinel at 11-12 (Jan. 2011).

⁸⁰ *Id.*

240. Al-Qaeda's doctrines concerning cooperation with other jihadists and the need for interoperability substantially mirrors that of Hezbollah, the Qods Force, and Regular IRGC. As a result, al-Qaeda, and its star pupil, the Taliban, often relied upon joint cell tactics to carry out their most spectacular attacks.

241. Al-Qaeda terrorists also regularly attacked U.S. forces alongside Taliban terrorists, including in some of the attacks that killed or injured Americans. For example, in the early 2000s, al-Qaeda's third-ranking member participated in attacks on Americans in Afghanistan alongside Taliban terrorists under the command of Sirajuddin Haqqani. As another example, on July 13, 2008, Taliban and al-Qaeda members jointly attacked a U.S.-Afghan outpost in Nuristan Province. Nine ISAF soldiers were killed in the attack.

242. In 2010, one terrorism scholar warned against drawing a bright line between al-Qaeda and the Afghan terrorist groups that it sponsored. In explaining the importance of "recogniz[ing] the link between al-Qa'ida and Afghan insurgent groups," he observed that a "policy focused on targeting al-Qa'ida – and not the Taliban, Haqqani Network, or other groups – would ignore one of the most egregious lessons from September 11."⁸¹

243. The U.S. government agreed. During the relevant timeframe, the U.S. government repeatedly stated that al-Qaeda and the Taliban acted together in a terrorist "syndicate," and warned against efforts to distinguish between them. Examples include:

- (i) Secretary of State Hillary Clinton, July 2009: "[W]e had an intensive strategic review upon taking office[.] And we not only brought the entire United States government together, but we reached out to friends and allies . . . [T]he result of that strategic review was to conclude that al-Qaeda is supported by and uses its extremist allies like elements

⁸¹ Seth G. Jones, *In the Graveyard of Empires: America's War in Afghanistan* at 332 (W.W. Norton & Co. 2010) ("*Graveyard of Empires*").

within the Taliban . . . to be proxies for a lot of its attacks . . . So the Taliban . . . [is] part of a kind of terrorist syndicate with al-Qaeda at the center[.]”⁸²

- (ii) Secretary of State Hillary Clinton, December 2009: “[W]e have increasingly come to see these organizations not as separate independent operators that occasionally cooperate with one another, but as part of a syndicate of terrorism. . . . [T]he level of operational cooperation, training, equipping, financing, has grown exponentially. And at the head of the table, like an old Mafia kind of diagram, sits al Qaeda.”⁸³
- (iii) Secretary of Defense Robert Gates, January 2010: “Defense Secretary Robert M. Gates said yesterday that Al Qaeda was using proxy terrorist groups to orchestrate attacks in . . . Afghanistan as part of a broader strategy to destabilize the region. In a news conference held after two days of meetings with Indian officials, Gates said Al Qaeda had formed a ‘syndicate’ of terrorist groups with Taliban factions in Afghanistan and Pakistan . . . ‘What we see is that the success of any one of these groups leads to new capabilities and a new reputation for all,’ Gates said. ‘A victory for one is a victory for all.’ US intelligence officials have said that jihadi groups in the region are cooperating more closely than ever . . . Gates said all of the factions were working under the umbrella of Al Qaeda.”⁸⁴
- (iv) Secretary of Defense Robert Gates, May 2010: “The other concern we have . . . is the creation of the syndicate of terrorist organizations that are working with each other, al Qaeda, the Taliban in Pakistan, the Taliban in Afghanistan, the Haqqani Network. There are five or six of these groups that are now really working together and a success for one is a success for all . . . And so this problem has become more complex as these groups have gotten closer and cooperated operationally in a way that we really haven’t seen, I think, significantly before 2007, 2006.”⁸⁵
- (v) Under Secretary of Defense for Policy Michele Flournoy, April 2011: “We view al Qaeda, Haqqani, the Taliban, these are all part of a syndicate of groups that help each other. The Pakistanis tend to make finer distinctions between them – you know, not being . . . tolerant to some, like al Qaeda, but otherwise tolerating others. We are trying to work with them to shift that perspective and shift that calculus.”⁸⁶

244. Al-Qaeda’s interdependence and joint venture with its affiliates in Afghanistan and Pakistan continued throughout the period in which Plaintiffs were killed and injured. As two

⁸² *Sec. of State Hillary Clinton*, NBC News: Meet the Press (July 26, 2009).

⁸³ S. Hr’g 111-479, at 24.

⁸⁴ *Gates Casts Qaeda As Terror Syndicate*, Wash. Post (Jan. 21, 2010), 2010 WLNR 1263055 (“*Gates Casts Qaeda As Terror Syndicate*”).

⁸⁵ *John King Presents: Full Interview with Secretary of Defense Robert Gates*, CNN (May 8, 2010), 2010 WLNR 27823364.

⁸⁶ *Hindustan Times, Pakistan Must Meet Certain Expectations on Counter-Terrorism* (Apr. 22, 2011).

journalists noted in 2016, the U.S. military’s relative success against al-Qaeda neither eliminated al-Qaeda nor broke apart its Syndicate: Afghanistan’s southern and eastern provinces remained a “hub of Afghan insurgents and [the] al-Qaeda-led terrorist syndicate.”⁸⁷ Similarly, as two terrorism scholars explained in a 2018 book, “[t]he Taliban still retain[ed] a close alliance with al-Qaeda,” which represented “the worst possible scenario for terrorism.”⁸⁸

245. Today, Afghanistan is a safe haven for al-Qaeda under the control of the “Islamic Emirate of Afghanistan.”⁸⁹

246. The Taliban promised U.S. negotiators that they would sever their alliance with al-Qaeda and kick them out of Afghanistan. That was a lie, and they have done the exact opposite since their victory. Indeed, al-Qaeda’s continuing fusion with the Taliban, including its Haqqani Network, was amply demonstrated after the fall of the U.S.-allied government there to the terrorists, when a litany of high-level al-Qaeda terrorists publicly traveled back, media retinue in tow, to their ancestral haunts in Afghanistan for the “conquering hero” photo-op.

2. Sirajuddin Haqqani (Al-Qaeda and Taliban)

247. From 9/11 through today, al-Qaeda’s terrorist enterprise benefited from al-Qaeda operatives who were “polyterrorists,” *i.e.*, al-Qaeda terrorist operatives who *also* simultaneously served as a terrorist operative for one or more al-Qaeda affiliates. By design, al-Qaeda

⁸⁷ Ayaz Ahmed & Dr. Faisal Javed, *Pakistan And SCO: Opportunities for Pakistan*, Asian Defence J. (Aug. 31, 2016), 2016 WLNR 25890108.

⁸⁸ Walter Laquer and Christopher Wall, *The Future of Terrorism* 153 (St. Martin’s Press 2018) (“Laquer and Wall, *Future of Terrorism*”).

⁸⁹ Plaintiffs categorically reject, in the strongest possible terms, any suggestion that the self-proclaimed “Islamic Emirate of Afghanistan” is a lawful government or anything other than terrorists. Plaintiffs recognize, however, that these terrorists – who remain a Foreign Terrorist Organization (in the case of al-Qaeda and the Haqqani Network) or Specially Designated Global Terrorist (in the case of the Taliban), now exercise territorial control over Afghanistan.

operatives were often members of other Pakistan-based al-Qaeda affiliates, most commonly, the Haqqani Network and Lashkar-e-Taiba. Typically, al-Qaeda's and the Haqqani Network's polyterrorist operatives or agents served the group's transnational terrorist activities in support of the attack campaign against Americans in Afghanistan. Former assistant Treasury secretary for terrorist finance Juan C. Zarate explained in 2013:

Treasury's [counter-terror] strategy ... aimed at targeting networks of key financial actors and nodes in the terrorist support system. The point was ... to make it harder for individuals who were financing terrorists to access the formal financial system. Our analyses therefore focused on the networks of actors and institutions providing the financial backbone to terrorist enterprises. Interestingly, we found that there were all-purpose financiers who would give to multiple causes—"polyterror" supporters.⁹⁰

248. Since the mid-2000s, Sirajuddin Haqqani was – and remains today – the signal example of an al-Qaeda “polyterrorist” operative who killed Americans. Sirajuddin Haqqani was the son of bin-Laden's long-standing ally, mentor, and protector, Jalaluddin Haqqani. By 2008, Sirajuddin Haqqani was simultaneously: (1) a senior al-Qaeda operative, leader, and attack planner, who served as the most important member of al-Qaeda's military council (essentially, its terrorist planning committee); (2) the Haqqani Network's top operative, attack planner, and leader; and (3) a senior leader of the Quetta Shura Taliban, which would eventually make him its number two leader (Deputy Emir).

249. Sirajuddin Haqqani's father, Jalaluddin Haqqani, was the most iconic Islamist terrorist in Afghanistan and Pakistan after bin Laden (and a far bigger deal there than bin Laden prior to 9/11). Sirajuddin grew up observing his father Jalaluddin play a leadership role coordinating the efforts of more than half a dozen separate Islamist insurgent groups that had all

⁹⁰ Juan C. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* 41 (Public Affairs 2013) (“Zarate, *Treasury's War*”).

united in an alliance to attack Soviet forces in Afghanistan to drive the Soviet Union out. Like the phenomenon of the children of professional coaches going into coaching themselves because they grew up marinating in it and becoming great coaches as a result, Sirajuddin's unparalleled biography and personal networks made him the hub of al-Qaeda and Taliban terror.

250. On February 29, 2008, the U.S. State Department designated Sirajuddin Haqqani a Specially Designated Global Terrorist for "acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States" and the U.S. Congress specifically identified Sirajuddin Haqqani as "the overall leader of the Haqqani Network as well as the leader of the Taliban's Mira shah Regional Military Shura" in 2012.⁹¹

251. When the U.S. Treasury Department designated Sirajuddin Haqqani's uncle Khalil Al-Rahman Haqqani as a SDGT, it noted that he "has also acted on behalf of al-Qa'ida and has been linked to al-Qa'ida military operations."⁹² The Treasury Department likewise has repeatedly recognized links between Haqqani Network leaders and al-Qaeda.

252. Sirajuddin Haqqani facilitated al-Qaeda members' efforts to join and fight with the Haqqani Network and the rest of the Taliban. According to U.S. intelligence officers, Sirajuddin Haqqani acts as a member of al-Qaeda's military council. U.S. officials have described him as al-Qaeda's top facilitator in Afghanistan.

253. Other than Osama bin Laden, Sirajuddin Haqqani was the single most important al-Qaeda leader since 9/11. By joining al-Qaeda management, Sirajuddin achieved a level of

⁹¹ Public Notice, *In the Matter of the Designation of Sirajuddin Haqqani, aka Sirajuddin Haqqani, aka Siraj Haqqani, aka Siraj Haqqani, aka Saraj Haqqani, aka Saraj Haqqani, as a Specially Designated Global Terrorist Pursuant to Section 1(b) of Executive Order 13224, as Amended*, 73 Fed. Reg. 12,499 (Mar. 7, 2008); Pub. L. 112-168, 126 Stat. 1299, § 2(a)(8) (Aug. 10, 2012).

⁹² Press Release, U.S. Dep't of Treasury, *Treasury Targets the Financial and Support Networks of Al Qa'ida and the Taliban, Haqqani Network Leadership* (Feb. 9, 2011).

interoperability and cohesion between al-Qaeda and the Taliban, including its Haqqani Network, that greatly magnified the lethality of the terrorists' campaign.

254. Sirajuddin Haqqani was also, like his father Jalaluddin Haqqani, famous for his pragmatism in defense of his extremism. Sirajuddin was willing to do deals and make trades with people, groups, and governments whom he may otherwise wish to kill if the deal in question made it more likely that al-Qaeda and the Taliban, including its Haqqani Network, could kill Americans in Afghanistan.

255. Sirajuddin Haqqani was the most important transnational Syndicate leader and played a vital role in harmonizing the various strategies and tactics, as well as promoting network efficiencies. Thus, for example, if a Qods Force "security" operative needed secure travel into Paktika Province (a Haqqani Network stronghold), the Qods Force terrorist could contact someone from the Haqqani clan and make the necessary arrangements.

256. When Plaintiffs were attacked, Sirajuddin Haqqani, and the al-Qaeda and Taliban organizations he led, promoted deep cooperation amongst al-Qaeda, the Taliban (including its Haqqani Network), and the IRGC (including Hezbollah and the Qods Force).

257. When Plaintiffs were injured between August 2017 and 2019, Sirajuddin Haqqani served as the top Syndicate "polyterrorist" responsible for coordinating key transnational-facing aspects of the Syndicate's terrorist campaign in Afghanistan and, in coordinating with other al-Qaeda and affiliated terrorists. Each of the below attack campaigns or types constituted an act of international terrorism committed by al-Qaeda, the Taliban, including its Haqqani Network, that was aided by Hezbollah, the Qods Force, and Regular IRGC.

- (i) **Kabul Attack Network Attacks.** Sirajuddin Haqqani planned and authorized the Syndicate attacks that targeted Kabul – which Sirajuddin Haqqani personally viewed as a tactical priority – that were committed by joint al-Qaeda/Taliban (including Haqqani

Network)/Lashkar-e-Taiba cells known as the Kabul Attack Network, including such joint cell's IED and suicide bomb attacks in Kabul and the surrounding provinces.

- (ii) **Fertilizer Bomb Attacks.** Alongside al-Qaeda, Sirajuddin Haqqani planned and authorized al-Qaeda's fertilizer bombing campaign, including, but not limited to, al-Qaeda's and the Haqqani Network's strategy for:
 - a. sourcing fertilizer;
 - b. purchasing and transporting fertilizer;
 - c. operating al-Qaeda bombmaking factories hosted at Sirajuddin's personal network of joint al-Qaeda-Haqqani Network terrorist camps in Pakistan; and
 - d. deploying fertilizer bombs as IEDs and suicide bombs to attack Americans in Afghanistan.
- (iii) **Suicide Bomber Attacks.** Sirajuddin Haqqani planned and authorized al-Qaeda's suicide bombing campaign, including, but not limited to, al-Qaeda's and the Haqqani Network's shared strategy for:
 - a. planning the targets for suicide bomber attacks in Afghanistan;
 - b. sourcing suicide bombers through al-Qaeda's and the Haqqani Network's long-standing allies, Lashkar-e-Taiba and Jaish-e-Mohammed; and
 - c. coordinating the "suicide bomber infrastructure" of camps, madrassas, ratlines, and safehouses, which relied heavily upon al-Qaeda and Haqqani Network resources and polyterrorists like Sirajuddin.
- (iv) **Kidnapping Attacks.** Sirajuddin Haqqani planned and authorized kidnappings in Kabul.
- (v) **Transnational Terrorist Finance and Logistics.** Sirajuddin Haqqani planned and authorized al-Qaeda's and the Taliban's, including its Haqqani Network's, transnational terrorist logistics, including, but not limited to:
 - a. al-Qaeda and the Taliban's, including its Haqqani Network's, transnational rackets necessary to the success of their:
 - i. criminal funding efforts, (e.g., money laundering, protection rackets, and tax fraud);
 - ii. fundraising and money movement, e.g., diaspora donations, banking relationships;

- iii. “tax” collection from the criminal underworld of their diaspora globally, e.g., logistics, communications in the U.A.E., Pakistan, Afghanistan, and Europe; and
 - b. al-Qaeda’s and the Haqqani Network’s transnational-operations and activities in Afghanistan, Pakistan, and the U.A.E. as they relate to smuggling or logistics, both of which have always ranked as top Haqqani Network specialties.
- (vi) **Coordination Between FTOs.** Sirajuddin Haqqani led two FTOs (al-Qaeda and the Haqqani Network) and was responsible for, or supervised those who were responsible for (like his brother Anas) managing al-Qaeda’s and the Taliban’s (including its Haqqani Network’s) relationships with a broad international alliance of allied terrorists, including, but not limited to:
 - a. Hezbollah, the Qods Force, and Regular IRGC;
 - b. the Pakistani Taliban, a member of the Syndicate;
 - c. Lashkar-e-Taiba, a member of the Syndicate; and
 - d. Jaish-e-Mohammed, a member of the Syndicate.

258. For more than a decade, and continuing through to today, Sirajuddin Haqqani was wanted by the FBI for his involvement in numerous acts of terror against Americans (he still is).

259. Even though he was (and remains) an FBI-Most-Wanted mass murderer with a reputation for savagery that was extreme even by Islamist standards, the *New York Times*’s editorial board shamefully elected to publish an op-ed authored by Sirajuddin himself, titled “What We, the Taliban, Want,”⁹³ on February 20, 2020. Sirajuddin’s op-ed was pure terrorist propaganda designed to persuade an American audience that the Taliban, including its Haqqani Network, had turned a more “inclusive” and “peaceful” page. Other than its title and the fact that Sirajuddin wrote it, the *Times* opinion piece was propaganda and of no value.

⁹³ Sirajuddin Haqqani, *What We, the Taliban, Want*, New York Times (Feb. 20, 2020).

260. Along with his brothers, who were also (and remain) key Haqqani Network leaders, as well as al-Qaeda operatives and/or agents, Sirajuddin Haqqani personally spearheaded the terrorists’ successful campaign on Kabul in August 2021.

261. Today, Sirajuddin Haqqani serves as the terrorist who is responsible for the “Islamic Emirate of Afghanistan’s”⁹⁴ borders and guns, while his brothers have responsibilities relevant to intelligence and information.

3. The Taliban, Including Its Haqqani Network

262. The Taliban is a Sunni Islamic terrorist organization comprised originally of former mujahideen fighters who had expelled the Soviet Union from Afghanistan.

263. The Haqqani Network is the most radical part of the Taliban. While Plaintiffs address each separately, they are part of the same organization (i.e., the Taliban).

i. The Taliban

264. In 2002, the U.S. designated the Taliban and its leader Mohammed Omar as Specially Designated Global Terrorists. President Bush found that these designations guarded against “grave acts of terrorism and threats of terrorism committed by foreign terrorists.”⁹⁵

265. On December 26, 2007, Congress enacted a law declaring that, for purposes of “section 212(a)(3)(B) of the Immigration and Nationality Act, . . . the Taliban shall be

⁹⁴ Plaintiffs refuse to recognize the legitimacy of the self-proclaimed “Islamic Emirate of Afghanistan,” but recognize that these terrorists, who remain FTOs (in the case of al-Qaeda and the Haqqani Network) and SDGTs (in the case of the Taliban), now exercise complete territorial control of a nation.

⁹⁵ Exec. Order No. 13,268, 67 Fed. Reg. 44,751 (July 3, 2002).

considered to be a terrorist organization.”⁹⁶ As a State Department official explained, the U.S. government treats the Taliban “as a Foreign Terrorist Organization for immigration purposes.”⁹⁷

266. At all relevant times, the U.S. government viewed the Taliban as a terrorist group, not as the legitimate armed force of any nation.

267. The Taliban’s principal goal has long been to expel Americans from the country and undermine the democratically elected government of Afghanistan. To that end, the Taliban attacked U.S. forces from 2001 through 2020, and achieved its objective in 2021.

268. At all relevant times, the Taliban used threats of terrorist violence to extract protection money from international companies doing business in Afghanistan. Such threats were particularly frequent in (though not limited to) geographic areas of Taliban control. By 2006, the Taliban had achieved control of wide swaths of southern and eastern Afghanistan, and by 2009 it had installed “shadow” governments in 33 of Afghanistan’s 34 provinces. It leveraged that control into protection payments. As an anticorruption investigator working for the U.S. House of Representatives explained, it was “long-standing business practice within Afghanistan to use your control of the security environment in order to extort payment from those who want to operate within your space, whether it’s construction of a cellphone tower, a dam, or running trucks.”⁹⁸ The Taliban perfected that practice by threatening contractors’ businesses until (and sometimes even after) they met the terrorists’ financial demands.

⁹⁶ Consolidated Appropriations Act of 2007, § 691(d), Pub. L. No. 110-161, 121 Stat. 1844, 2365.

⁹⁷ U.S. Dep’t of State, *Senior Administration Officials on the Terrorist Designation of the Haqqani Network* (Sept. 7, 2012).

⁹⁸ Karen DeYoung, *Afghan Corruption: How To Follow The Money?*, Wash. Post (Mar. 29, 2010) (“*Afghan Corruption*”), 2010 WLNR 26719956.

269. The Taliban's threats presented companies with a choice: alert the government and seek the U.S. military's assistance while investing in legitimate security to protect their projects, or instead save time and money by paying the Taliban to direct its attacks elsewhere. One American executive whose company conducted business in Afghanistan described the decision as "'whether you'd rather pay \$1,000' for Afghans to safely deliver a truck, even if part of the money goes to the insurgents, or pay 10 times that much for security provided by the U.S. military or contractors."⁹⁹ Contractors, including Defendants, typically chose the former option. The owner of one logistics subcontractor described the prevailing mentality: "'I pay the Taliban not to attack my goods, and I don't care what they do with the money,' he said laughing. 'If you don't, the next day your property is attacked and destroyed.'"¹⁰⁰

270. Companies, including Defendants, rationalized their payments to the Taliban by framing them as a necessary cost of business. But the payments were unnecessary – even from the standpoint of Defendants' own security needs – and counterproductive. In reality, they chose to pay not because of any reconstruction imperative, but because it served their financial interests. As an adviser to the Afghan Interior Ministry explained, "the costs of enabling the Taliban's protection racket outweigh the benefits of any reconstruction that might come out of it."¹⁰¹ He noted that "it might be more convenient to pay off the Taliban, and it might be faster," but it "both prolongs the war and feeds criminality, which in turn turns more people against the

⁹⁹ *Id.*

¹⁰⁰ Hamid Shalizi, *Afghan Firms Said To Pay Off Taliban With Foreign Cash*, Reuters (Oct. 13, 2010) ("*Afghan Firms Pay Off Taliban*").

¹⁰¹ Aryn Baker, *How The Taliban Thrives* at 51, Time Magazine (Sept. 7, 2009) ("*How The Taliban Thrives*").

government.”¹⁰² By diverting money to insurgents, the payments lowered the projects’ quality and undermined whatever counterinsurgency benefits they might have otherwise delivered.

ii. The Haqqani Network

271. The Haqqani Network is a Sunni Islamic terrorist organization that has been operating in Afghanistan since the 1970s. It was founded by Jalaluddin Haqqani and is now led by his son, Sirajuddin Haqqani. The Haqqani Network is a member of the Syndicate, has been a part of the Taliban for decades, and is closely allied and interdependent with al-Qaeda.

272. On September 19, 2012, the U.S. State Department designated the Haqqani Network as an FTO.

273. The U.S. designated multiple Haqqani leaders as SDGTs. As previously mentioned, the U.S. designated Sirajuddin Haqqani as an SDGT in 2008 and, in 2010 and 2011, the followed up by designating three other Haqqanis—Nasiruddin, Khalil Al-Rahman, and Badruddin—as fundraisers and commanders of the Haqqani Network. By February 2014, the U.S. had designated fourteen leaders in the Haqqani Network under Executive Order 13224.¹⁰³

274. The Haqqani Network was especially active in the southeastern parts of Afghanistan, particularly in the Paktia, Paktika, and Khost (“P2K”) Provinces. It also developed a significant presence in the surrounding Provinces of Kabul, Logar, Wardak, Ghazni, and Zabul.

¹⁰² *Id.* at 51.

¹⁰³ It is not uncommon for the U.S. government to issue a terrorism-related designation years, and sometimes even decades, after a terrorist suspect first becomes internationally notorious for his or her role enabling terror. This ordinarily does not reflect uncertainty about whether someone was a terrorist, only the uniquely cumbersome inter-agency legal and diplomatic process, which often stretches years, that the U.S. government completes before most terrorism-related designations including, on information and belief, each designation identified in this Complaint.

Because of the Haqqani Network's longstanding tribal connections to the southeastern region of Afghanistan, the Taliban often acts through the Haqqani Network in those areas.

275. The Haqqani Network's influence is not limited to one Afghan region. There is also significant overlap between the broader leadership of the Taliban and the Haqqani Network. Sirajuddin Haqqani has been a member of the Taliban's governing council since at least 2010. Since 2015, he has been the Deputy Emir of the Taliban, the Taliban's second in command. Working alongside al-Qaeda, the Haqqani Network has overseen the Taliban's terrorist attacks on U.S. and Coalition forces in Afghanistan. For example, after September 11, Jalaluddin Haqqani effectively served as the Taliban's secretary of terrorism and planned many of the Taliban's attacks on U.S. forces in the early days following the overthrow of the Taliban government while sheltering al-Qaeda leadership at the time.

276. Both Sirajuddin and Jalaluddin Haqqani have confirmed that the Haqqani Network operates as part of the Taliban. The Taliban has rejected claims that the Haqqani Network is separate from the Taliban.

277. The Haqqani Network has significant links to al-Qaeda, dating back to the 1980s when Osama bin Laden established a training camp for his nascent terrorist group in Haqqani-controlled territory. After September 11, the Haqqanis provided sanctuary to bin Laden.

278. The Haqqani Network's close relationship with al-Qaeda and other terrorist groups has helped grow the modern terrorist Syndicate operating in Afghanistan. In furtherance of that goal, the Haqqani Network provides protection to al-Qaeda so that it can launch attacks in Afghanistan and plan acts of international terrorism abroad. Senior Haqqani Network officials also have publicly indicated that the Haqqani Network and al-Qaeda are one. And in July 2008, Jalaluddin Haqqani's son—18-year-old Muhamman Omar Haqqani—was killed alongside a top

al-Qaeda commander in southeast Afghanistan. The Haqqani Network also maintains training camps and safehouses that have been used by al-Qaeda and Taliban operatives.

279. Along with al-Qaeda, the Haqqani Network jointly operated and conducted al-Qaeda's CAN fertilizer bomb campaign in Afghanistan, and Haqqani Network agents, operatives, and fronts, including Haqqani Network co-conspirators Fatima and Pakarab, were vital to sourcing every component necessary for the Syndicate to execute its CAN fertilizer bomb campaign at a nationwide scale throughout Afghanistan.

280. The Haqqani Network ordinarily managed the Taliban's transnational terrorist finance and logistics operations and often aided al-Qaeda's transnational terrorist finance and logistics activities. When doing so, the Haqqani Network used its network of agents, operatives, and fronts in the U.A.E. as an alias for its fellow Syndicate terrorists. As explained by Haqqani Network expert Gretchen Peters, the Haqqani Network's interlocking financial support of other Syndicate members through cross-border transactions included, but was not limited to: (1) managing the Taliban's international narcotics enterprises, and repatriating¹⁰⁴ profits back to the Taliban to fund attacks against Americans in Afghanistan; (2) raising funds for al-Qaeda and the Taliban from commercial activities overseas and repatriating those monies back to al-Qaeda and the Taliban to fund attacks against Americans in Afghanistan; and (3) committing transactions through known Haqqani Network operatives, agents, or fronts around the world, including, but

¹⁰⁴ By "repatriating profits," Plaintiffs refer to the process through which al-Qaeda, the Haqqani Network, and their allies, used their operatives, agents, fronts, or partners to launder illicit overseas income, convert such funds into U.S. Dollars from their original currency (*e.g.*, Russian Rubles), and transfer such cleansed money back to the terrorist group's designated "controller," *e.g.*, Altaf Khanani, who then manages the money and disperses it consistent with the needs and request of the terrorist group. Such "repatriation" by al-Qaeda, the Taliban (including the Haqqani Network), and their allies occurred through their use of operatives, agents, fronts, and partners throughout the world.

not limited to, such Haqqani Network assets in the U.A.E., Afghanistan, Pakistan, Russia, Central Asia, Germany, Italy, Cyprus, and other key sites in Europe, the Middle East, and Asia, all of which directly funded al-Qaeda and Haqqani Network operations that supported their shared terrorist campaign against Americans in Afghanistan.

281. The Treasury Department determined that the Haqqani Network regularly used its transnational terrorist finance activities to fund multiple al-Qaeda-affiliated Syndicate members simultaneously. For on February 9, 2011, the Treasury Department designated Syndicate operatives, Said Jan Abd Al-Salam and Khalil Al-Rahman Haqqani (Jalaluddin's brother), as SDGTs to "target the financial and support networks of al-Qa'ida, the Taliban and the Haqqani Network leadership."¹⁰⁵

282. By 2010, CAN fertilizer sourced from Pakistan was "one of the most coveted substances in a Taliban bomb-maker's arsenal" and served as "the basic ingredient of the Taliban's roadside bombs,"¹⁰⁶ and the Syndicate had developed a sophisticated end-to-end logistics chain for the sourcing, manufacture, and distribution of al-Qaeda CAN fertilizer bombs. By 2011, "U.S. military officials believe[d] the Haqqani [N]etwork" was "working closely with [CAN fertilizer] suppliers," *e.g.*, Fatima, "to help smuggle the fertilizer across the border."¹⁰⁷

283. By the time it was designated as an FTO on September 19, 2012, the Haqqani Network, working closely with al-Qaeda, had grown and refined the Syndicate's CAN fertilizer bomb logistics chain in Afghanistan and Pakistan for more than five years.

¹⁰⁵ *Id.*

¹⁰⁶ Alex Rodriguez, *Bribes Keep Taliban Flush with Explosives*, L.A. Times (May 8, 2010), 2010 WLNR 9039604.

¹⁰⁷ Aamer Madhani, *Tensions With Pakistan Rise Over Bomb Ingredient*, National Journal Daily (Jul. 6, 2011), 2011 WLNR 13371684.

4. The Kabul Attack Network

284. The Kabul Attack Network was an operational manifestation of the terrorist syndicate led by al-Qaeda and the Taliban, including its Haqqani Network. Specifically, the Kabul Attack Network was a set of terrorist cells, which included members from each of the terrorist groups involved in the Syndicate and focuses on attacks against targets in Kabul and extending outward into the provinces of Logar, Wardak, Nangarhar, Kapisa, Kunar, Ghazni, and Zabul.¹⁰⁸ It was active around key waypoints and transit routes on the way to Kabul, including Wardak, Ghazni City, and areas of Logar Province.

285. The Kabul Attack Network's forward deployed terrorists were drawn from joint cells comprised of al-Qaeda, the Taliban (including its Haqqani Network), Lashkar-e-Taiba, and Jaish-e-Mohammed, each of whom participated in Kabul Attack Network attacks and contributed personnel and resources to such attacks. For each group, the Kabul Attack Network's attacks were the most important, or among the most important, priorities of the Syndicate's entire terrorist campaign since 9/11, and thus received special focus from each Syndicate member.

286. Attacks committed by the Kabul Attack Network were committed jointly by a combined cell comprised of these terrorists. By the same token, funding for any of the involved terrorist groups contributed to the Network's attacks.

287. The Kabul Attack Network was responsible for high profile and/or mass casualty attacks on Americans in Kabul and the surrounding areas that relied upon fertilizer bombs, suicide bombers, kidnappers, or insider attacks.¹⁰⁹

¹⁰⁸ Bill Roggio, *Karzai Assassination Plotters Part of Kabul Attack Network*, Long War J. (Oct. 5, 2011).

¹⁰⁹ Bill Roggio, *Afghan Intel Captures Taliban Commander Involved In Targeting 'Foreigners' In Kabul*, Long War J. (Mar. 31, 2015).

288. On January 24, 2010, the Afghan government accused al-Qaeda of specifically planning the Kabul Attack Network's CAN fertilizer bomb attacks in Kabul, which the Syndicate delivered via IED and suicide bomb.

289. Sirajuddin Haqqani, the dual-hatted al-Qaeda-Taliban terrorist, planned and authorized every attack committed by the Kabul Attack Network, working with local commanders like Mullah Dawood. to execute the Kabul Attack Network's attacks. As a result, at all relevant times, the Kabul Attack Network's attacks were planned and authorized by at least one FTO (al-Qaeda), and after September 19, 2012, Kabul Attack Network attacks were planned and authorized jointly by two FTOs (al-Qaeda and the Haqqani Network).

290. According to an ISAF public affairs officer, the "Haqqani Network [was] deeply entrenched in the Kabul Attack Network specifically with the facilitation of weapons and fighters into the area south of Kabul in Logar and Wardak."¹¹⁰ Additionally, senior Haqqani leaders operating from their traditional strongholds often planned and executed terrorist attacks by the Kabul Attack Network, sometimes even giving tactical advice during attacks.

291. The Kabul Attack Network's attacks were funded and logistically supported by al-Qaeda, the Taliban (including its Haqqani Network), Lashkar-e-Taiba, Jaish-e-Mohammed, and D-Company access to terrorist finance in Afghanistan, Pakistan, and worldwide, including through their conspiracy with Hezbollah, the Qods Force, and Regular IRGC. Thus, terrorist finance that flowed to any of these groups aided Kabul Attack Network attacks.

¹¹⁰ Bill Roggio, *Senior Taliban Commander Killed in Eastern Afghanistan*, Long War J. (Aug. 20, 2010).

C. In Furtherance Of The Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Operated As An Integrated Transnational Terrorist Organization With A Common Doctrine, Strategy, Financial Structure, Logistics Structure, And Command-And-Control

1. The IRGC's Transnational Terrorist Strategy, Doctrine, And Tactics Emphasizes The Deployment Of Joint Cells Of Terrorists Led By Hezbollah, Funded And Resourced By The Qods Force, And Supported By Local Iranian Terrorist Proxies

292. Hezbollah, the Qods Force, and Regular IRGC, have long followed a common terrorist strategy and doctrine, which deploys common tactics across every component of the IRGC (regular, Hezbollah Division, and Qods Force) – including the use of Hezbollah as the cell leader and Qods Force as cell funder and logistician – and every geography in which the IRGC or any of its proxies operate.

293. The IRGC adheres to an integrated global terror strategy, and follows the same rules for terrorist tradecraft, out of a recognition that the IRGC and its proxies were likely to always suffer from a resource deficit, which meant that the intelligent deployment of its human assets was paramount because unlike, say, China, the IRGC did not have limitless resources or an enormous pool of human capital from which to draw. Given these “equipment and logistical constraints, Hezbollah – with the guidance of Iranian advisors – adopted a doctrine of guerrilla warfare against the Israeli occupation.”¹¹¹

294. The Joint Cell approach is the foundation of the IRGC's terrorist doctrine and the cornerstone of the Hezbollah Division's entire terrorism “business model” when, as in most use cases, the Hezbollah Division and Qods Force are being deployed outside of Iran, or are being deployed inside of Iran but specifically to target Americans, e.g., to torture an American hostage being held in Iran, or to plan for a raid targeting Americans from a site in Iran.

¹¹¹ Lindemann, *Laboratory of Asymmetry*.

2. Hezbollah, The Qods Force, And Regular IRGC Follow Common Terrorist Techniques, Tactics, And Procedures And Use The Same Terrorist Tradecraft To Ensure Concealment And Cover Worldwide

295. “Tradecraft” refers to the methodologies and philosophies of engaging in covert operations (including killings) and general espionage. Terrorists and clandestine intelligence operatives both practice tradecraft.

296. The tradecraft rules that govern Hezbollah, the Qods Force, and Regular IRGC are ironclad, inflexible, widely known, and universally applied worldwide, befitting the IRGC’s status as the world’s largest, most globally distributed, professionalized transnational terrorist organization. IRGC tradecraft emphasizes concealment and cover above all other operational imperatives.

297. While Islamist terrorists and western intelligence officials do not agree on much, they concur on the core doctrinal point that the two *absolute requirements* for nearly any successful operation by terrorists or intelligence operatives are **(i) Concealment**, i.e., something or someone that protects something (or someone) else from being identified; and **(ii) Cover**, i.e., something that provides protection or shelter to someone otherwise at risk.

298. Amongst counter-terror professionals, it is axiomatic that “cover” and “concealment” are a necessary ingredient to any successful long-term terrorist finance and logistics strategy that depends upon commercial transactions to facilitate terror.

299. Nearly everything a terrorist does requires cover and concealment in some form: meeting with cell members, communicating with leadership, surveilling targets, traveling across an international border to attend a training camp, and so on.

300. Since the IRGC’s founding, the security doctrine followed by Hezbollah, the Qods Force, and Regular IRGC, have consistently emphasized cover and concealment as the

essential aspect of any successful terrorist operation in light of the unique, violent, and affirmative need for the IRGC to “go on offense” and attack Americans abroad.

301. Hezbollah, the Qods Force, and Regular IRGC adheres to cover and concealment as the two most important principles in terrorist tradecraft for a simple reason: from inception, and ever since, the IRGC’s security policy was specifically built on paranoid, antisemitic, Islamist aggression that explicitly targeted America (sometimes by name, sometimes in code), and posited that an alliance between Christians (Americans) and Zionists (Israelis) was bent on taking over the Middle East and defiling Islam, and thus each member of the IRGC (including Hezbollah and the Qods Force) must always be attacking Americans, and always focusing specifically on targeting the United States for terror.

302. The IRGC (including Hezbollah and the Qods Force) was built purposely for the specific task of attacking America and Israel in order to protect Iran’s Islamic Revolution by staying on a perpetual state of “offense,” i.e., a never-ending campaign of terror against Americans and their allies in the Middle East and around the world designed to strike the “infidels” on their own ground – rather than fight on Iranian soil – via terrorist attacks usually carried out through a Joint Cell approach that outsources much of the violence to local IRGC proxies, but always under the control of Hezbollah and the Qods Force.

303. Hezbollah, the Qods Force, and Regular IRGC, adhered to the above-described security policy for the purported purpose of preventing “Christians” and “Zionists” from overrunning the Middle East, ending Iran’s Islamic Revolution, and forcibly converting every Muslim in the world to Christianity and Judaism.¹¹² At all times, and continuing to this day, the

¹¹² The last point reflects a particularly ominous aspect of the theological doctrine underpinning the “security” doctrine adhered to by the IRGC, including Lebanese Hezbollah and Qods Force.

Iranian Shareholders with whom ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) conspired, i.e., fronts for the IRGC (including Hezbollah and the Qods Force), have adhered to this doctrine.

304. The ability of Hezbollah, the Qods Force, and Regular IRGC, to depend upon the reliability of its covers – corrupt corporate partners – was essential to the conspiracy’s ability to obtain a vast storehouse of high-tech American smartphones, network computing technologies.

i. Concealment

305. Every principle of terrorist tradecraft practiced by Hezbollah, the Qods Force, and Regular IRGC, begins with concealment. While every Foreign Terrorist Organization, like the IRGC, prioritizes concealment, few have more practical experience accomplishing concealment. And, from experience, organizations grow (for good or ill). Hezbollah, the Qods Force, and Regular IRGC, have decades of terrorist experience and is the most experienced, practiced terrorist organization in the world today with respect to concealment, a status it earned in the 1990s and has maintained ever since.

306. Under the “security” doctrine universally practiced at all times by the IRGC, including Hezbollah and Qods Force, IRGC terrorists are taught as a matter of terrorist tradecraft that, if they are faced with a choice between: (a) possibly blowing the concealment of an IRGC, including Hezbollah and Qods Force, cover, plot, operative, or transaction, and exposing the IRGC asset in question to capture by the hated “Great Satan,” i.e., the U.S., and “Little Satan,” i.e., Israel, detection by the “Christians,” i.e., the United States, and/or the “Zionists,” i.e., Israel, or (b) simply lying, cheating, stealing, defrauding, burning, kidnapping, or murdering your way

Under the theology espoused by Iran’s radical clerics, a Muslim conversion to Christianity (forcibly or not) is viewed as an apostasy, the worst possible thing someone can do, and the worst possible fate that could befall someone in return.

out of the problem, there is ***no choice at all*** for any terrorist who is a member of Hezbollah, the Qods Force, and Regular IRGC. For such a terrorist, IRGC doctrine commands them to maintain concealment of the asset to prevent discovery by the U.S.

307. To be clear, Plaintiffs do not allege that IRGC, including Hezbollah and Qods Force, have any discretionary authority in the immediately preceding hypothetical. ***Just the opposite:*** a well-trained terrorist following the tradecraft of Hezbollah, the Qods Force, and Regular IRGC, is ***affirmatively compelled*** to lie, cheat, defraud, kidnap, torture, rape, and murder – whatever is necessary to maintain concealment – as a religious duty, analytically no different from other pious acts because the crime in question was purportedly in service of the Islamic Revolution and the IRGC’s holy mandate to “preserve” the Revolution since 1979 by conducting waves of terror campaigns coordinated by Hezbollah’s External Security Organization.

308. The IRGC’s obsession with preserving concealment underpins this case. Because Hezbollah, the Qods Force, and Regular IRGC, prioritizes concealment above all else, an IRGC operative would never truthfully reveal their “security”-related status – i.e., that they were a terrorist operative assigned to the IRGC’s Hezbollah Division’s External Security Office or through the IRGC’s Qods Force and currently on a mission.

309. The ordinary “use case” for most Foreign Terrorist Organizations, including the IRGC, assumes that the FTO’s forward deployed terrorists worked in-country with local proxies to attack Americans nearby, and that the FTO’s operatives are often highly motivated, but isolated and poorly resourced. IRGC (including Hezbollah and Qods Force) tradecraft emphasizes the intense vulnerability of Iranian terrorists considering America’s military power,

intelligence capabilities, surveillance prowess, dominance of the global financial system through New York banks, and status as the world's most technologically advanced country.

310. IRGC (including Hezbollah Division and Qods Force) "security" operatives (i.e., terrorists) were (and are) paranoid about their concealment and went to extreme lengths to preserve it.

311. When a forward deployed intelligence operative or terrorist is operating under concealment, as most do, one key challenge involves how to develop reliable partners outside of the terrorist group (e.g., a partner who helps Hezbollah but is not himself a member) or intelligence service (e.g., a source).

312. Hezbollah, the Qods Force, and Regular IRGC, do not lightly accept foreigners in their terrorist "circle of trust." And the IRGC did not do so here.

313. To earn – and keep – the trust of Hezbollah, the Qods Force, and Regular IRGC, the IRGC insisted that MTN Group and MTN Dubai, and on information and belief, ZTE Corp. and Huawei Co., sign the same IRGC template, in which each Defendant pledged to facilitate the "security" operations of the IRGC, i.e., Hezbollah and Qods Force attacks against Americans worldwide.

314. IRGC concealment doctrine emphasizes an "Orbit" strategy under which the IRGC, including its Hezbollah Division and the Qods Force, structures transactions so that the IRGC is behind one side, one step removed, but fully in control. This IRGC tradecraft is designed to give the IRGC, and its corrupt corporate and financial enablers, the ability to falsely claim that the IRGC did not directly benefit from an otherwise suspect transaction because the counterparty himself was not a member of the IRGC.

315. In 2020, NATO confirmed the IRGC’s “Orbit” strategy in an analysis by Monika Gill, a defense scholar who closely studied how the IRGC deploys communications technology to facilitate anti-American terror,¹¹³ that NATO published in *Defence Strategic Communications*, “[t]he official journal of the NATO Strategic Communications Centre of Excellence.”¹¹⁴

316. According to Ms. Gill’s study of the IRGC’s communications technology strategies, the IRGC’s practices while exercising control of Iran’s heavy construction industry show the IRGC’s “Orbit” strategy as being part of their terrorist tradecraft, because the entire point of the strategy is to enable a future accomplice – like a company that gets caught red-handed – to protest that there is no direct linkage between them and the IRGC:

The IRGC-CF is comprised of a complex network of Orbit 1 companies and Orbit 2 companies. In Orbit 1 companies, the IRGC-CF is directly represented on the board of directors, whilst in Orbit 2 companies, there ***appears to be no direct representation and therefore, seemingly no links*** to the IRGC-CF. Whilst Orbit 2 companies appear independent of the IRGC, they maintain ties to the directly affiliated companies, and therefore remain under indirect IRGC influence. Baharahn Gostar Kish for example, is an information technology and communications company that has no formal links to the IRGC-CF, with no IRGC members on the board of directors. However, two board members represent Baharahn and Mowj Nasr Gostar, which are both Orbit 1 companies, ***meaning that the company still effectively falls under the IRGC economy.***¹¹⁵

317. Ms. Gill’s analysis leaves no doubt as to the true nature of Defendants’ counterparties. Indeed, it compels the conclusion that, even now, Defendants’ representations merely further the IRGC’s conspiracy. Simply put, it is textbook IRGC terrorist tradecraft to structure deals that are designed to route value to the IRGC even when both sides to the

¹¹³ Gill, *Capitalism, Communications, and the Corps*, at 88.

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 101-102 (emphasis added).

transaction are *not* IRGC, which is a long-standing IRGC practice from transactions involving companies the IRGC effectively controls even when the IRGC is not a party to the transaction.

318. NATO would not have published Ms. Gill’s factual findings concerning MTN Irancell unless they were reasonable.¹¹⁶

ii. Cover

319. The IRGC’s terrorist doctrine emphasizes the reliance upon charities, corporations, and endowments, and other ostensibly “civilian” or “economic” entities as covers for Hezbollah, the Qods Force, and Regular IRGC.

320. In recognition of the central role of cover to IRGC doctrine, the IRGC created Unit 400 within the Qods Force. As one regional newspaper explained in 2021:

Unit 400 has a network of facilitators and proxies, including elements in organized crime syndicates. These individuals collect information, make preliminary logistical preparations, and carry out operations if necessary. These individuals sometimes are trained inside Iran and sometimes in the Quds Force’s training camps across the globe. Unit 400 has various front companies that both provide cover and money for this terrorist entity to operate. Two companies, Arash Zoobin, and Aria Navid, are used to secretly transfer weapons for Unit 400. Besides, the IRGC uses its vast network of front companies, religious or charitable organizations around the world to recruit facilitators.¹¹⁷

321. As a consequence, the IRGC, including its Hezbollah Division and the Qods Force, relied upon the importance of using crooked corporate partners to provide “cover” to facilitate, among other things: **(i) illicit financial transactions to acquire and distribute U.S.**

¹¹⁶ NATO would only publish a lengthy article replete with complex factual assertions if the professional staff at NATO, on behalf of NATO, believed the article: (1) accurately characterized the facts to avoid misleading the contemplated primary audience or making any assertions that are implausible, e.g., a government official working for NATO to defend the U.S. and Europe from, inter alia, terrorism; (2) offered reasonable opinions worthy of consideration by responsible parties, e.g., analyzing how NATO should respond to the IRGC takeover of MTN Irancell and Telecommunication Company of Iran (“TCI”); and (3) strengthened NATO’s ability to fight terrorism, as that was NATO’s primary mission for the two decades after 9/11.

¹¹⁷ Shahriar Kia, *Global Terrorist Activities Of The Iranian Mullah Regime*, Weekly Blitz (Bangladesh) (Dec. 4, 2021), 2021 WLNR 39679934.

Dollars, e.g., laundering and recycle U.S. Dollar-denominated drug profits to finance Hezbollah operations; **(ii) illicit purchases of embargoed American technology**, e.g., bulk purchasing thousands of black market secure American mobile phones; **(iii) illicit movement of terrorist operatives**, e.g., a Hezbollah attack planner whose need to visit Europe requires a visa supplied by a credible front company; **(iv) illicit safe havens**, e.g., a fictitious company used as cover for an al-Qaeda safehouse in Afghanistan; and **(v) illicit cache sites**, e.g., Hezbollah attack planner whose need to visit Europe requires a visa supplied by a credible front company.

iii. Slush Funds For “Off-Books” Terrorist Finance

322. Given the IRGC’s programmatic emphasis on deception and the use of “slush funds,” core IRGC doctrine emphasizes that the IRGC, including its Hezbollah Division and the Qods Force, must draw a substantial portion of the funds, arms, personnel, and logistical support for anti-American terrorism globally from “off-books” sources, with the Bonyad Mostazafan being the most notorious – and important – terrorist slush fund of them all.

323. Moreover, “all the IRGC's economic activities are monitored only by internal IRGC auditors and that the corps pays no taxes.”¹¹⁸

iv. Corruption As Terrorist Tactic And Tool

324. The terrorist tradecraft practiced and taught by Hezbollah, the Qods Force, and Regular IRGC, have long used corruption, bribery, kickbacks, “taxes,” and protection money as a core strategy to facilitate terrorist attacks against Americans in Afghanistan, Iraq, and elsewhere through: (1) terrorist finance, including raising funds, concealing funds, converting funds to U.S. Dollars (the currency of choice for all terrorists), and moving the Dollars to the

¹¹⁸ Rasool Nafisi, *Iran’s Revolutionary Guard Has A Lot To Lose*, Radio Free Europe Documents (Sept. 18, 2009), 2009 WLNR 18604289.

necessary terrorist cell; (2) terrorist logistics, including acquiring the embargoed technologies necessary to improve the bombs, rockets, communications, and surveillance capabilities necessary to kill or kidnap Plaintiffs; and (3) terrorist freedom of movement, including securing visa and other government papers necessary to a plot, bribing law enforcement to prevent the roll-up of a cell, and the like.

325. Decades of Hezbollah operations, investigations, and prosecutions confirm how Hezbollah, the Qods Force, and Regular IRGC, converted income from the transnational corruption economy for terror, including, but not limited to, examples ranging from Hezbollah's role in the Lebanese banking system (Hezbollah dominated it), to Hezbollah's sponsorship of narcotics trafficking (Hezbollah serves as an elite global management consulting company for narcotraffickers), to Hezbollah's involvement in transnational organized crime worldwide (where Hezbollah serves as both partner, client, and management consultant).

326. By 2004, Hezbollah, the Qods Force, and Regular IRGC, had spent more than two decades developing and refining their shared tradecraft, networks, strategies, and tactics relevant to using corruption as a tool for terror. As a result, Hezbollah, the Qods Force, and Regular IRGC, already had a purpose-built transnational infrastructure enabling to convert the profits derived from the "corruption economy" in one country into attacks in that country or others.

v. Required Donations (*Khums*) From All IRGC Members

327. Shiite theological traditions call for donations (*khums*), usually equal to twenty percent (20%) of a person's income on every transaction, to support the cause. The IRGC, however, has twisted this religious tradition, like tithing in Christianity, into something else.

328. Under the longstanding IRGC doctrine that Hezbollah teaches to Iranian proxies like Jaysh al-Mahdi, the IRGC emphasizes the need to consistently collect donations (or taxes) as something that is universally required from all profit-generating activities and transactions –

without exception – including, but not limited to, profits generated through official business, criminal rackets, bribery and kickbacks, and a broad array of other illicit cash flow schemes. The IRGC’s “no exceptions” rule ensures that the terrorist have an administratively simple scheme (analogous to a terrorist flat tax), which ensures ease of implementation, and comports with the broader IRGC emphasis on its terrorists and proxies embracing administrative simplicity in their jihad.

329. Under IRGC doctrine, *khums* donations are mandatory on multiple different transaction types, all of which ultimately flow back to fund the IRGC, including its Hezbollah Division and the Qods Force. *First*, if income flows through and IRGC-controlled front (i.e., MTN Irancell) to the IRGC shareholders behind that front (i.e., the IRGC, including its Hezbollah Division and the Qods Force), the respective shareholders provide a donation to the others. Thus, for example, if MTN Irancell flowed through \$100 million to the IRGC, one may infer that the IRGC would, in turn, donate approximately twenty percent (20%) – \$20 million – to its Hezbollah Division and the Qods Force in order to export Iran’s Islamic Revolution abroad through anti-American terror.

330. *Second*, if a member of the IRGC – or a cutout acting on their behalf – receives a substantial economic benefit, such as a \$400,000 bribe, IRGC doctrine mandates that the bribe recipient kickback, mafia-style, twenty percent of their income to the IRGC. Thus, for example, an IRGC member (or cut-out) who received a \$400,000 bribe could ordinarily be expected to kickback \$80,000 to the IRGC, or likely meet the same fate that would befall a captain in the Gambino crime family who tried to keep a nearly half-million-dollar score from the Don (death).

3. **Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Tradecraft And Doctrine Has Historically Relied On Fronts, Operatives, Agents, Cut-Outs, And Orbits To Fund, Arm, And Operationally Aid IRGC Terrorist Proxy Attacks Against Americans**

331. The terrorist tradecraft and doctrine of Hezbollah, the Qods Force, and Regular IRGC, reflects a long and notorious history of relying on fronts, operatives, and agents to obtain funding, weapons, and operational support to benefit the IRGC's, including the Qods Force's, terrorist operations and Anti-American proxies around the world, most of all Hezbollah.

332. On February 10, 2010, the U.S. Treasury Department announced additional IRGC front-related designations and stated that Hezbollah, the Qods Force, and Regular IRGC, were using illicit commercial transactions to bolster Iran's terrorist enterprise:

The U.S. Department of the Treasury [] took further action to implement existing U.S. sanctions against Iran's [IRGC] by designating an individual and four companies affiliated with the IRGC ... "As the ***IRGC consolidates control over broad swaths of the Iranian economy, ... it is hiding behind companies ... to maintain vital ties to the outside world,***" said Under Secretary for Terrorism and Financial Intelligence Stuart Levey. "Today's action ... will help ***firms worldwide avoid business that ultimately benefits the IRGC and its dangerous activities.***" ... The U.S. has previously acted against the IRGC and the IRGC-Qods Force for their involvement in proliferation and terrorism support activities, respectively. In joint actions on October 25, 2007, the State Department designated the IRGC, under E.O. 13382, for having engaged, or attempted to engage, in proliferation-related activities, and ***Treasury designated the IRGC--Qods Force pursuant to E.O. 13224 for providing material support to ... terrorist organizations.*** ...¹¹⁹

333. On August 3, 2010, the U.S. Treasury Department announced additional IRGC- and Qods Force-related terrorist designations that bolstered the U.S. message that the "IRGC and IRGC-QF" provided "Support for Terrorist Organizations," including Hezbollah, and relied upon illicit commercial transactions to fund and arm the IRGC-led terror campaign against Americans:

¹¹⁹ U.S. Treasury Dep't, *Treasury Targets Iran's Islamic Revolutionary Guard Corps* (Feb. 10, 2010) (emphasis added).

The U.S. Department of the Treasury announced [] a set of designations targeting the Government of Iran's support for terrorism and terrorist organizations, including Hizballah ... Iran is the primary funder of Hizballah and has long been recognized as the most active state sponsor of terrorism. Today's designations expose Iran's use of its state apparatus – including the Islamic Revolutionary Guard Corps-Qods Force – and state-run social service organizations to support terrorism under the guise of ... economic development ...

IRGC and IRGC-QF Support for Terrorist Organizations:

The IRGC-QF is the Government of Iran's primary arm for executing its policy of supporting terrorist and insurgent groups. The IRGC-QF provides material, logistical assistance, training and financial support to militants and terrorist operatives throughout the Middle East and South Asia. It was designated by Treasury pursuant to E.O. 13224 in October 2007 for its support of terrorism.

The Government of Iran also uses the Islamic Revolutionary Guard Corps (IRGC) and IRGC-QF to implement its foreign policy goals, including, but not limited to, *seemingly legitimate activities that provide* cover for intelligence operations and *support to terrorist and insurgent groups. These activities include economic investment ... implemented by companies and institutions that act for or on behalf of, or are owned or controlled by the IRGC and the Iranian government.*

- ... In Iraq, the Government of Iran trains, equips, and funds Iraqi Shia militant groups.
- In the Levant, the IRGC-QF continues to support designated terrorist groups such as Hizballah...[,] the largest recipient of Iranian financial aid, training, and weaponry; and Iran's senior leadership has cited Hizballah as a model for other militant groups.¹²⁰

334. On December 21, 2010, the U.S. Treasury Department announced additional IRGC-related designations, and stated once again that IRGC, including Hezbollah and the Qods Force, relied upon illicit commercial transactions, including through the Bonyads like Bonyad Mostazafan, to facilitate Iran's terrorist enterprise:

The U.S. Department of the Treasury announced [] a set of designations targeting the financial networks of the Islamic Revolutionary Guard Corps (IRGC) ... Today's actions further expose the continued engagement of the IRGC ... in illicit activities and deceptive behavior.

¹²⁰ U.S. Treasury Dep't, *Fact Sheet: U.S. Treasury Department Targets Iran's Support for Terrorism Treasury Announces New Sanctions Against Iran's Islamic Revolutionary Guard Corps-Qods Force Leadership* (Aug. 3, 2010) (emphasis added).

“[T]he IRGC ... [is a] major institutional participant[] in Iran’s illicit conduct and in its attempts to evade sanctions. We will therefore continue to target and expose [its] networks,” said Under Secretary for Terrorism and Financial Intelligence Stuart Levey. ... The IRGC continues to be a primary focus of U.S. and international sanctions against Iran because of the central role it plays in Iran’s ... support for terrorism The U.S., UN, EU, Japan, South Korea and others have all targeted the IRGC for sanctions because of this illicit activity. With the IRGC’s expanding influence and control over broader segments of the Iranian economy ... increasing numbers of Iranian businesses are subsumed under the IRGC’s umbrella and identified with its illicit conduct.

... Iranian bonyads are opaque, quasi-official organizations controlled by key current and past government officials and clerics. Bonyads receive benefits from the Iranian government but are not required to have their budgets publicly approved. They account for a significant portion of Iran’s non-petroleum economy. ... Treasury has designated 14 IRGC-affiliated individuals and entities since June 2010 for facilitating Iran’s nuclear and ballistic missile program or support for terrorism.¹²¹

335. On June 23, 2011, the U.S. Treasury Department announced additional IRGC-related designations that reinforced the U.S. message that illicit transactions with IRGC commercial fronts directly aided terrorism against Americans by Iranian terrorist proxies:

Treasury Targets Commercial Infrastructure of IRGC, Exposes Continued IRGC Support for Terrorism. Today, the U.S. Department of the Treasury took action to designate ... Iranian commercial entities ... owned by [IRGC] ... The IRGC continues to be a primary focus of U.S. and international sanctions against Iran because of the central role it plays in all forms of Iran’s illicit conduct, including Iran’s ... support for terrorism ... As Iran’s isolation has increased, the IRGC has expanded its reach into critical sectors of Iran’s economic infrastructure – to the detriment of the Iranian private sector – ***to generate revenue and conduct business in support of Iran’s illicit activities.*** Today’s actions target core commercial interests of the IRGC, while also undermining the IRGC’s ability to continue using these interests to facilitate its ... illicit conduct. ... The IRGC has a growing presence in Iran’s financial and commercial sectors and extensive economic interests ..., controlling billions of dollars in corporate business. Given its increased involvement in commercial activity, imposing financial sanctions on commercial enterprises of the IRGC has a direct impact on revenues that could be used by the IRGC to facilitate illicit conduct.¹²²

¹²¹ U.S. Treasury Dep’t, *Fact Sheet: Treasury Designates Iranian Entities Tied to the IRGC and IRISL* (Dec. 21, 2010).

¹²² U.S. Treasury Dep’t, *Fact Sheet: Treasury Sanctions Major Iranian Commercial Entities* (June 23, 2011) (emphasis added).

D. In Furtherance Of The Conspiracy, Hezbollah, The Qods Force, And Regular IRGC Managed A Transnational Network Of Terrorist Finance, Logistics, Operations, And Communications Cells To Fund, Arm, Logistically Sustain, And Facilitate Attacks On Americans In Afghanistan

1. United States

336. Hezbollah, the Qods Force, and Regular IRGC, rely upon a global network of cells, operatives, cover companies, and allied criminals in the corporate world (like Defendants) and the criminal world (like narcotraffickers and transnational crime organizations).

337. Hezbollah, the Qods Force, and Regular IRGC, operated the conspiracy in the same manner as a multinational corporation, seeking to leverage geographic efficiencies, networks, and distributed competencies to maximize the lethality of the conspiracy's terrorist campaigns against Americans in Afghanistan, Iraq, Yemen, Syria, Europe, Pakistan, and elsewhere. This section briefly outlines how Hezbollah, the Qods Force, and Regular IRGC, leveraged terrorist finance, logistics, technical and communications support from around the world to directly aid the terror campaign against Americans in Afghanistan.

338. **American Technologies.** Hezbollah, the Qods Force, and Regular IRGC depended upon the IRGC's ability to access technologies, markets, and systems that were found exclusively in the United States to execute key parts of the conspiracy. Simply put, they needed as much access to America as possible to kill as many Americans as possible.

339. Hezbollah, the Qods Force, and Regular IRGC relied upon American-designed, protected, manufactured, and/or assembled technologies, including but not limited to, mobile phones, smartphones, enterprise level servers, computer networking technologies, and software, because they have been the gold standard from 9/11 through today. No other country made a credible version of a competing device, that is available for sale to the public as opposed to their own "security" agencies at any point in time between 2001 and 2022, e.g., enterprise level

servers and secure encrypted smartphones that can access the full panoply of universally sought-after “apps”), at any point in time between 2001 and 2022.

340. **American Markets.** Hezbollah, the Qods Force, and Regular IRGC relied upon in-person and online sales markets in the United States, including but not limited to currency markets (relying upon the U.S. Dollar as the IRGC’s preferred currency) technology markets (relying on U.S. goods as the IRGC’s preferred technology source), financial markets (relying on U.S. financial markets because U.S. banks have connectivity to the 50+ countries on six continents in which Hezbollah and the Qods Force operates), labor markets (relying on skilled laborers, particularly information technology consultants, to service the IRGC’s illicitly acquired U.S. technologies), and black markets (relying on the ability to acquire some of the above items that can only be purchased in the U.S.).

341. In every instance, Hezbollah, the Qods Force, and Regular IRGC depended upon its ability to access American markets at home to kill Americans abroad because such U.S. markets have unique power to set the terms and pricing for the world, and were often also the only location where Hezbollah, the Qods Force, and Regular IRGC could acquire a key item in the covert manner needed under the IRGC’s terrorist tradecraft. For example, the IRGC did not have the ability to source large amounts of U.S. Dollars or access state-of-the-art American technologies without the IRGC, or one of its corporate co-conspirators, reaching into the United States to further the conspiracy. This case concerns the various nodes and modalities by which the IRGC accomplished that.

342. **American Systems.** Hezbollah, the Qods Force, and Regular IRGC relied upon its ability to access certain financial, technical, and knowledge systems that were stored exclusively inside the United States. For example, the IRGC depended upon the ability of its

terrorist computer programmers to be able to access certain proprietary databases located inside of the United States in order to complete the design of a particular part necessary for a new type of bomb being developed by the IRGC.

2. U.A.E.; Iraq; Iran; Lebanon; Yemen; Syria; Afghanistan; Pakistan

343. From 9/11 through the present, attack planners, logisticians, and financiers for Hezbollah, the Qods Force, and Regular IRGC as well as nearly every other major Islamist terrorist group, including but not limited to al-Qaeda, the Taliban (including its Haqqani Network), and others, have relied upon the U.A.E., especially Dubai, as a logistical, financial, and operational hub, from which they could organize their terrorist campaigns in Iraq, Iran, Lebanon, Yemen, Syria, Afghanistan, and Pakistan.

344. With respect to the IRGC's terrorist campaign against Americans in Afghanistan, Iraq, Iran, Lebanon, Yemen, and Syria in furtherance of the IRGC's conspiracy, the U.A.E. served as a logistical, financial, and operational hub for the campaign, and the U.A.E. was functionally part of one interlocking geography of extreme terrorist finance and logistics risk and hub of activity,¹²³ comprised for purposes of the IRGC Shiite Terrorist Proxies' terror campaign of the U.A.E., Iraq, Iran, Lebanon, Yemen, and Syria.

345. With respect to the IRGC's terrorist campaign against Americans in Iraq, Iran, Lebanon, Syria, Europe, Afghanistan, and Pakistan in furtherance of the IRGC's conspiracy, the U.A.E. served as a logistical, financial, and operational hub for the campaign, and the U.A.E.

¹²³ For the avoidance of all doubt, the government of the U.A.E. was, and remains, an ally of the U.S. in the fight against terrorism. The terrorists' use of the U.A.E. as a hub was based on a range of other factors, including, but not limited to, geography, history, particular trading networks, transportation channels, and an advanced infrastructure for conducting transactions and moving goods and monies throughout the Middle East. The terrorists, like many multinational corporations, set up their regional headquarters in Dubai for these reasons.

was functionally part of one interlocking geography of extreme terrorist finance and logistics risk and hub of activity, comprised for purposes of the IRGC Syndicate Terrorist Proxies' terror campaign of the U.A.E., Iraq, Iran, Lebanon, and Syria.

346. Simply put, the terrorists did not respect the borders of any of these countries – other than Iran and Syria, with whom they were allied rendering the issue moot – and viewed the entire geography as one combined theater.

3. South Africa

347. Hezbollah, the Qods Force, and Regular IRGC have long operated openly and notoriously in South Africa. “Iran and South Africa have cooperated on a number of fronts in recent decades, including at the U.N., where South Africa has at times advocated for Iran” and “[t]he pair also have a military relationship.”¹²⁴

348. The IRGC's freedom of movement in South Africa is a legacy of Ayatollah Khomeini, who stood against the Apartheid regime while, unfortunately, the United States (for a time) did not.

349. For decades, Hezbollah, the Qods Force, and Regular IRGC leveraged Iran's historical feat of standing up to Apartheid, in much the same way that the Soviet Union exploited Jim Crow to undermine the America's image as a bastion of liberty during the Cold War. Both messages were effective.

350. Because of this unique Iranian-South African history, Hezbollah, the Qods Force, and Regular IRGC viewed South Africa as a veritable home away from home for the IRGC, as South Africa was one of the few major democracies to have abstained from joining the sanctions

¹²⁴ Nahal Toosi and Natash Bertrand, *Officials: Iran Weighing Plot To Kill U.S. Ambassador To South Africa*, Politico (Sept. 13, 2020).

regime against Iran and to afford the IRGC relatively unfettered freedom of movement. As a result, Hezbollah, the Qods Force, and Regular IRGC operated clandestine fundraising, logistics, and operations networks in South Africa for decades.

351. In an interview with *Politico*, American intelligence officials confirmed on background that “[t]he Iranian government [] operate[d] clandestine networks in South Africa,” “and has had a foothold there for decades.”¹²⁵ “In 2015, Al Jazeera and The Guardian reported on leaked intelligence documents that detailed an extensive secret network of Iranian operatives in South Africa.”¹²⁶

352. According to leaked documents from the South African intelligence service, Hezbollah and the Qods Force operate cells in South Africa showing “confirmed” links between Iranian operatives in overseas embassies and “terrorists.”

353. In or about 2020, American intelligence services detected that Hezbollah, the Qods Force, and Regular IRGC was planning a terrorist attack in South Africa to kill the U.S. ambassador to South Africa as retaliation for the killing of Qassem Soleimani in January 2020.

354. Hezbollah’s choice of South Africa as the potential attack site is revealing, as the terrorists had the chance to survey all the world to choose the best location to kill an American ambassador. As *Politico* noted, the U.S. ambassador to South Africa “may also [have] be[en] an easier target than U.S. diplomats in other parts of the world, such as Western Europe, where the U.S. ha[d] stronger relationships with local law enforcement and intelligence services.”¹²⁷

¹²⁵ *Id.*

¹²⁶ *Id.*

¹²⁷ *Id.*

4. Europe

355. Europe has long been a hub for terrorist finance, logistics, and operational support for Hezbollah, the Qods Force, and Regular IRGC as well as al-Qaeda, the Taliban, including its Haqqani Network, and their allied Syndicate terror partners in Afghanistan and Pakistan. Europe's proximity to many of the attack theaters and ease of travel make it a key site for the terrorist campaign.

5. The Americas

356. The IRGC, through Hezbollah and the Qods Force, maintains a substantial presence in the Americas, including, but not limited to, in Venezuela, Colombia, Paraguay, and other nations.

357. Hezbollah and the Qods Force maintained operational, finance, and logistics cells throughout multiple nations in the Americas, through which Hezbollah operated an array of money-making criminal schemes, e.g., narcotics trafficking, in order to repatriate money back to the terrorist campaign.

358. Hezbollah and the Qods Force support the terrorist campaign in the Middle East from their cells in the Americas. Indeed, that is the purpose of the cells far from Hezbollah's home in Beirut – cash and logistics flow for the terror campaign.

6. Southeast Asia

359. The IRGC, through Hezbollah and the Qods Force, maintains a substantial presence in Southeast Asia.

360. Hezbollah and the Qods Force maintain operational, finance, and logistics cells throughout multiple Southeast Asian nations, including Malaysia and Singapore.

361. Hezbollah and the Qods Force support the terrorist campaign in the Middle East from their Southeast Asian cells. Indeed, that is the purpose of the cells far from Hezbollah's home in Beirut – cash and logistics flow for the terror campaign.

IV. THE CONSPIRACY DEPENDED UPON THE CO-CONSPIRATORS' ROBUST ACCESS TO U.S. TECHNOLOGY, U.S. DOLLARS, AND U.S. PERSONS TO CARRY OUT ATTACKS AGAINST AMERICANS IN THE MIDDLE EAST

A. After The U.S. Invasions Of Afghanistan And Iraq, Hezbollah, The Qods Force, And Regular IRGC Concluded That They Needed To Revolutionize Their Access To U.S. Technologies Through Corrupt Corporate Partners

362. In the decade prior to the U.S. invasion of Iraq in 2003, the technological gap between IRGC, including Hezbollah and Qods Force, "security" operatives, on the one hand, and the counter-terrorist forces hunting them (and protecting against their threats), on the other, grew from large (in the 1980s) to vast (in the 1990s).

363. By 2003, the tech-gap between the "security" operatives deployed by Hezbollah, the Qods Force, and Regular IRGC on the one hand, and U.S. counter-terrorists, law enforcement, and intelligence officers, on the other, was so vast it was as if Americans and the IRGC "security" operatives targeting them lived on two different technological planets: "Earth 1" and "Earth 2".

364. After the fall of Saddam Hussein in 2003, U.S. personnel in the Middle East practiced their counter-terror tradecraft on **Earth 1** where Americans wielded 24/7 surveillance powers that were difficult to overstate, possessed unparalleled intelligence networks, and had real-time data analytic abilities that played a key role in reducing the threat of Islamist terror. The single most important contributor to America's dominant technological edge – and greatest barrier to the IRGC's terrorist conspiracy succeeding – was the fact that America could count on achieving close, reliable, and robust cooperation from the iconic, well-capitalized, and patriotic

American telecommunications and network computing companies, which have historically worked as responsible partners with the U.S. government to prevent terror.

365. Meanwhile, on **Earth 2** – where IRGC “security” operatives practiced their tradecraft – the world was upside down and terrifying. A sloppy phone call could result in a precision American airstrike a few minutes later. An errant text message could enable the “Great Satan” to take down a Joint Cell. A carelessly documented transaction could reveal an important laundering scheme. Most of all, the “security” operatives of Hezbollah, the Qods Force, and Regular IRGC were caught in a digital cage from which they could not carry out their religious, and constitutionally prescribed duty – attack and kill Americans.

366. The IRGC knew that the U.S. telecom and network computing industry would not solve their problem – if anything, the American industry would only widen the gap even more between the IRGC and the Americans it wanted to kill. For decades, large U.S. telecom and network computing companies have been reliable partners of the U.S. government with respect to reducing the threat from terrorism. Indeed, the anti-terrorism track record of America’s telecommunications and network computing companies has been among the best of any industry anywhere in the world.¹²⁸

367. This matters because the robust commitment of American telecom and network computing companies to anti-terrorism compliance was known to the IRGC (and all other industry participants), which meant that the terrorists knew they would be unable to count on their normal strategy for illicitly acquiring something – pay a bribe, threaten extortion, engage in fraud – because none of those strategies held the promise of working at the industrial scale that

¹²⁸ Plaintiffs are not aware of any federal criminal terrorism-related prosecutions, civil Anti-Terrorism Act allegations, or analogous anti-terrorism matter brought by any government against any such companies.

Hezbollah, the Qods Force, and Regular IRGC required for their global terrorist conspiracy against Americans.

368. By 2003, the IRGC knew that its operatives would never be able to sustain the global terrorist conspiracy it had planned against America after 9/11 unless the IRGC could find a way to break out of the digital detention cell that was effectively created by the walls of compliance offered by America's telecommunications and network computing companies.

369. Hezbollah ordinarily serves as the IRGCs illicit procurement agent of choice for a litany of reasons including, but not limited to, deniability, cultural affinities, and the presence of a Lebanese diaspora relatively evenly dispersed around the world, upon which Hezbollah, like most Islamist groups, heavily relies.

370. By 2003, the IRGC had tasked Hezbollah with solving a riddle: how do they, the terrorists, establish the reliable, secure, and covert pipeline that they need to illicitly acquire the tens of thousands of state-of-the-art American smartphones and network computing technologies *each year* necessary to sustain their decades-long, global terrorist campaign against America?

371. The answer? Identify potential multinational corporate partners who would be willing to provide the technology they needed.

372. As the IRGC spun up its transnational terrorist conspiracy, its leadership worked with Hezbollah and the Qods Force to develop a comprehensive plan to revolutionize their respective terrorist capabilities to prepare for their anticipated decades-long terrorist campaign against Americans throughout the Middle East. To accomplish the object of the conspiracy – ejecting the United States from the entire Middle East through a campaign of terror – the terrorists had five critical requirements.

373. *First*, the IRGC and its terrorist allies needed a generational upgrade in the security of their computer systems and network technologies, especially the state-of-the-art American servers that were *the* condition precedent for the IRGC's ability to execute its Revolution in Terrorist Affairs, and without which, the IRGC's efforts would be less effective, would be less efficient, would be more expensive, and would produce, ultimately, fewer dead Americans. Given the sheer scale of the IRGC's terrorist conspiracy targeting Americans in Afghanistan, Iraq, Syria, Yemen, Israel, and elsewhere, even marginal improvements in IRGC computing power translated to more plots being shared, more fundraising solicitations, more recruits, and ultimately, more attacks.

374. *Second*, the IRGC and its terrorist allies needed a reliable, replenishable, untraceable source of suppliers for illicit high-quality American-manufactured mobile phones sold in markets inside the United States, and then illegally reexported to eventually flow through the Qods Forces logistics channels – as intended – before reaching Hezbollah, who relied upon American phones to coordinate Iran's global terrorist conspiracy, including its campaign against Americans in Afghanistan and Iraq.

375. Given the transnational nature of the IRGC's terrorist conspiracy, Hezbollah, the Qods Force, and the leadership of terrorist proxies like Jaysh al-Mahdi (in Iraq) and the Taliban (in Afghanistan), faced a simple, but potentially fatal, problem confronting their post-9/11 terrorist enterprise against America: how to facilitate the free movement of key terrorist leaders, attack planners, fundraisers, and logisticians between the various hubs of the conspiracy, e.g., a senior Hezbollah operative who shuttles from Beirut (where Hezbollah is based), to Syria (where Hezbollah and the IRGC maintain a listening post), to Baghdad (where Hezbollah led Joint Cells

targeting Americans), and then to Tehran (where the IRGC is based). This isn't the plot of a spy movie: it describes the ordinary travel patterns of thousands of IRGC terrorists each year.

376. While most people think of false identification papers as being the most indispensable thing to freely traveling, that's analog thinking. The IRGC understood that, in the modern terrorist era, their operatives were at one critical disadvantage: Hezbollah and the Qods Force lacked the industrial scale supply, and re-supply, of secure mobile phones, and therefore Hezbollah and the Qods Force were at an enormous disadvantage because their operatives were hemmed in, with Americans in Afghanistan and Iraq, and unable to move for fear their phones were compromised by the Americans (as they likely were).

377. Worse, the IRGC lacked any easy solutions because America dominated the mobile phone industry and was not open for business to the IRGC. Shut off from the U.S. marketplace, the IRGC was unable to build their own phones and unwilling to place the lives of their most prized operatives – the people who led Joint Cells and coordinated operations – in the hands of the junky, unreliable, and often prone-to-failure mobile phones being made outside of the United States at the time.

378. Thus, the IRGC embarked on a comprehensive strategy designed to achieve its Revolution in Terrorist Affairs, obtain reliable industrial scale supplier relationships that could source American mobile phones, close the communications gap with the "Great Satan," and enhance the lethality of its global terrorist campaign against America. To do so, the IRGC needed to source tens of thousands of untraceable mobile phones *every year* to ensure the secure and untraceable communication lines between combined cells of Hezbollah, Qods Force, and local proxy terrorist allies operating in dozens of countries worldwide and, among other people,

their local organized crime allies (e.g., narco-traffickers), corrupt politicians (essential for things like passports and permits), and terrorist headquarters, as examples.

379. Unfortunately for Hezbollah, the Qods Force, and Regular IRGC who were responsible for the conspiracy's transnational logistics, weapons, financial, personnel flows, they could not source the tens of thousands of advanced American smartphones they needed every year with a few purchase orders on Bonyad Mostazafan's letterhead, because the terrorists were sanctioned. Even if the IRGC were not sanctioned, as a matter of IRGC terrorist tradecraft, lawful purchases of American phones inside U.S. markets by the precious Hezbollah or Qods Force assets inside the United States (for whom exposure was not to be risked lightly), while viable in small increments, was impossible at the commercial scale necessary for the conspiracy to succeed. Moreover, direct purchases by Hezbollah or Qods Force assets themselves would leave an evidentiary paper trail and risk the terrorists' operatives being rolled up by law enforcement or intelligence operatives – a potential catastrophe for Hezbollah, the Qods Force, and Regular IRGC.

380. Logically, that left the IRGC in a predicament. The IRGC could only satisfy its various operational requirements through the bulk acquisition of thousands of high-end American mobile phones every year but if the IRGC attempted to do so directly, even using IRGC front companies, the terrorist enterprise would not be nearly as effective or yield nearly as many American phones, because the black-market cell phone trade is a volume business where deals and goods must move rapidly. Thus, the IRGC needed front companies that offered the

agility, resources, global networks, and executives with willingness to aid the world's worst terrorists for profit.¹²⁹

381. Accordingly, the IRGC's ability to prosecute a global terrorist campaign against the United States required the services of corrupt multinational corporate partners, with deep resources, large logistics chains, and a willingness to conspire with anti-American terrorists. The following characteristics were key:

- (i) **New terrorist cash flow** generated by taking over a "civilian" company, to make it *easier* to illicitly acquire American technology (that's the point of being a cover) and make it *harder* for the IRGC's enemies to mobilize effective sanctions against the funding source (because IRGC apologists, like MTN Group, could publicly spread disinformation to undermine any pressure campaigns, as MTN Group did, and continues to do to this day);
- (ii) **Illicit acquisition of critical American technologies**, including secure American smartphones, computer networks, and sensitive dual-use American technologies to accomplish the IRGC's own Revolution in Terrorist Affairs; and the
- (iii) **Robust logistics capabilities** befitting the operation of Hezbollah, the Qods Force, and Regular IRGC as a multinational terrorist corporation that had a constant need to manage and rationalize the flow of illicit funds, arms, communications, narcotics, and personnel across six continents, all in support of the shared terrorist enterprise stretching from Syria to Iraq to Afghanistan.

382. At bottom, decrepit telecommunications, network computing, and associated technologies posed an immediate, and dire, threat to Iran's ability to kill as many Americans as possible in Afghanistan and Iraq because they were generations behind the United States on virtually every key class of communications and computing technologies necessary to sustain a modern transnational terrorist campaign stretching from Syria to Afghanistan.

¹²⁹ Because the global market for the sale of illegal American smartphones was vulnerable to law enforcement shocks that could rapidly suppress (temporarily) the supply chain – e.g., a raid in Detroit that removed one of the largest dealers from servicing the black market – it was imperative for the IRGC that its purchasing agents have the agility, financial resources, and global assets to source illicit American-exported cell phones in black markets worldwide, including, but not limited to, illicit cell phone markets on every continent but Antarctica.

383. The “Revolution in Military Affairs” or “RMA” refers to a widely accepted military hypothesis that emerged in the 1990s and posited that Western militaries needed to prepare for future asymmetrical threats by maximizing the technological gap between Western militaries and local hostile forces, e.g., IRGC proxies in Afghanistan, in order to achieve objectives such as increasing the speed with which forces can maneuver, increasing the flow of intelligence to troops, facilitating real-time information sharing amongst allied friendly forces, and promoting “interoperability” between the militaries of different nations, e.g., making sure that British forces in southern Iraq can communicate on the same channels as their American counterparts.

384. By early 2004, the IRGC’s terrorist conspiracy was in full bloom. Hezbollah, the Qods Force, and Regular IRGC had embraced its own take on the RMA, but repurposing the principles for use by Iran-backed terrorists (e.g., a Revolution in Terrorist Affairs). In particular, the IRGC concluded that it needed to overhaul the terrorists’ communications, computing, internet, and cyber capabilities to enable Iran to continue supporting attacks against Americans in Afghanistan and Iraq.

385. The IRGC had no choice but to seek American technology because America held the dominant position with respect to the world’s computers, mobile phones, servers, routers, and the like, and the IRGC understood that it needed to illicitly acquire vast amounts of embargoed American technologies to commit terrorist attacks.

386. By late 2004, the IRGC was desperate to upgrade its telecommunications because it understood that its ability to help kill and maim Americans at scale in Iraq, Afghanistan, and elsewhere depended upon the ability of its Hezbollah and Qods Force operatives, and their proxies to solve their American mobile phone access crisis. The IRGC’s terrorist proxy Jaysh al-

Mahdi was routed by U.S. forces twice that year. Moreover, the escalating gap between American counter-terrorists and IRGC “security” operatives, i.e., Hezbollah and Qods Force terrorists, threatened to eviscerate the ability of Hezbollah, the Qods Force, and Regular IRGC to facilitate terrorist violence against the United States in Afghanistan and Iraq.

387. Indeed, the IRGC watched, with escalating alarm, as its communications and computing gap widened, and threatened its ability to attack and kill Americans in Afghanistan and Iraq and, viewed the need to find a long-term technology supply fix as on par with Iran’s purported need to build a nuclear weapon and was one of the highest priorities of Hezbollah, the Qods Force, and Regular IRGC.

B. Hezbollah, The Qod Force, And Regular IRGC Addressed The Conspiracy’s Funding And Logistics Needs By Militarizing The Iranian Telecommunications Industry And Seizing Control Of Iran’s Largest Telecommunications Companies In Order To Acquire The Communications Technologies, Cash Flow, Logistical Support, Financial Management Support, Operational Support, Management Consulting Support, And Crisis Response Support From Corporate Partners Necessary To Sustain A Twenty-Year Terrorist Campaign Against Americans

388. In 2004, the IRGC embarked on a two-step solution. *Step One:* the IRGC seized Iran’s large state-owned telecom companies and converted them into tools of terrorist finance, logistics, propaganda, recruiting, and operations. As Ms. Gill explained, “just prior to [Mahmoud] Ahmadinejad’s election in 2005”:

Ayatollah Khamene’i issued a decree ... ordering 25% of state-owned assets to be privatised within 5 years. \$120 billion worth of government assets were sold ... Yet, the *largest purchaser of privatised government assets was the IRGC*, which received favourable terms from the Ahmadinejad regime. Under the *guise* of de jure privatisation, state-owned assets were *de facto militarised*.¹³⁰

¹³⁰ Gill, *Capitalism, Communications, and the Corps*, at 104 (emphasis added).

389. **Step Two:** the IRGC secured the agreement of complicit, corrupt telecommunications companies, including ZTE Corp., Huawei Co., and co-conspirators MTN Group and MTN Dubai, which were willing to do business with fronts for the IRGC's transnational terrorist logistics, technology, and financial enterprise and help the terrorists illicitly source the comprehensive suite of state-of-the-art American technologies that the IRGC determined were necessary to the ability of its own Revolution in Terrorist Affairs, so that Hezbollah and the Qods Force could do what they ended up doing: launch a devastating wave of violence against Americans throughout Afghanistan and Iraq.

390. The IRGC's two most important telecom front company targets were Irancell and TCI, and the IRGC quickly assumed full control of both companies, completely converting each to its terrorist enterprise.

1. MTN Irancell

391. In 2004, the IRGC negotiated with Turkcell, a mobile phone company based in Turkey, hoping Turkcell would be the corrupt corporate partner the IRGC required in order to extract a vast digital armory of embargoed American technologies. As negotiations progressed, however, Turkcell made it clear that they would not enable the IRGC's "security" agenda. Among other things, Turkcell refused to act as a communications technology logistics front for the IRGC. While Turkcell was willing to help build a modern Iranian phone system, it was not willing to provide direct "security" assistance to the IRGC.

392. MTN Group and MTN Dubai had no such scruples. Sensing weakness in the IRGC's negotiations with Turkcell, MTN Group and MTN Dubai hatched a comprehensive plan, which they internally called "Project Snooker," designed to steal the Irancell license from Turkcell – and the billions of dollars in profits that would flow to MTN Group and MTN Dubai thereafter. Ms. Gill explained the result:

the **IRGC asserted their role** in the communications economy through two significant developments in telecommunications infrastructure involving MTN Irancell and TCI. MTN Irancell was launched in 2005, at the start of Ahmadinejad's presidency, as a ... joint venture between ... MTN Group and the Iran Electronic Development Company (IEDC). A subsidiary company of the Iranian Ministry of Defence, IEDC maintained **close ties with the Revolutionary Guard**. **Following the IRGC's opposition** to foreign involvement in Iran's strategic telecommunications sector, IEDC negotiated 51% ownership of the MTN Irancell joint venture, ensuring that **the military had a majority stake in the newly formed telecommunications infrastructure**.¹³¹

393. In her article documenting how the IRGC converted MTN Irancell and TCI into tools of terrorist finance and logistics, published by NATO, Ms. Gill explained:

Communications infrastructure, particularly media and telecommunications licenses, are a source of state revenue. ... [T]he communications economy is lucrative for those involved. Ahmadinejad's regime faced a dichotomy between reaping the 'business benefits of a modern information infrastructure', whilst simultaneously preventing the communication of political criticism of the regime or of the broader Islamic revolutionary system. Therefore, communications infrastructure was treated as a political asset. Whilst the regime de jure separated telecommunications providers and regulators from the direct control of the Iranian state, de facto control was 'rarely surrendered by privatisation'. Khamene'i's Article 44 decree shows that the legal separation between state and assets allowed leaders to remain influential in the communications economy by appointing politically like-minded affiliates. By **militarising, rather than privatising the economy**, the regime transferred ownership from 'relatively transparent parts of the public sector to **other parts of the public sector shielded from public scrutiny**', such as the **Revolutionary Guard**. It is in this **fictional separation between the public and private sector in Iran that the invisible hand of the IRGC can be assessed**. **Power projection and realpolitik** remained central to the Guard's strategic thinking to the same extent as their ideological devotion.¹³²

394. The IRGC's takeover of MTN Irancell and TCI produced a financial windfall for Hezbollah, the Qods Force, and Regular IRGC. Ms. Gill explained that:

From a business perspective, the IRGC ... create[ed] a military-commercial complex in which the Guard benefitted from the construction of a perceived and persistent threat. ... Whilst publicly promoting rhetoric about national **security** and the defence of Shi'ite Islamic culture, the IRGC was **sustaining a military-commercial complex that benefited them financially**. The IRGC and the Iranian

¹³¹ Gill, *Capitalism, Communications, and the Corps*, at 105 (emphasis added).

¹³² Gill, *Capitalism, Communications, and the Corps*, at 108-109 (emphasis added).

communications economy maintained a *close partnership*, with both taking advantage of the articulation of a soft war. ...[T]here [was] a notably profit-driven motive to the Guard's economic involvement. ... the involvement of the IRGC in the communications economy under Ahmadinejad was reflective of an ideological, but also increasingly opportunistic Revolutionary Guard.¹³³

395. “[T]he IRGC became a moneymaking machine” after it deliberately blended the commercial and terrorist functions of MTN Irancell and TCI in order to ensure that Hezbollah, the Qods Force, and Regular IRGC could use MTN Irancell and TCI revenues to furnish off-books cash to, among other things, keep former members of Hezbollah, the Qods Force, and Regular IRGC on the IRGC's payroll. According to Ms. Gill,

The IRGC acts as a business fraternity within which members of the Guard can progress along a prescribed career path. Following active service, IRGC members are offered senior positions in state-affiliated media organisations and telecommunications networks *such as IRIB, TCI, and MTN Irancell*. *Accordingly, ‘no one ever leaves the IRGC’*; its senior officers are viewed as an Iranian ‘freemasonry’ and ‘Ivy League network’, signalling that the IRGC exceeds ideological devotion. ... When ‘privatising’ the national media and telecommunications infrastructure, the Ahmadinejad regime sold its majority stake to the IRGC, *blending its mission of national security with ‘investor profits’*. In holding senior economic positions in communications infrastructure companies and accruing profits, *the IRGC became a ‘moneymaking machine ...* The IRGC's opportunistic and exploitative involvement in the communications economy facilitated a system of military crony capitalism within Ahmadinejad's Iran. ... The IRGC *grew to depend on the communications economy to support the personal and financial endeavours of the Guard*, who valued safeguarding their own self-interest to the same extent as they valued safeguarding the revolution.¹³⁴

396. In sum, according to Ms. Gill, “the IRGC as an institution was reliant on the communications economy as a source of capital gain” and “the IRGC used the fictional separation between the public and private sectors in Iran to facilitate its rise as an economic

¹³³ Gill, *Capitalism, Communications, and the Corps*, at 110-111 (emphasis added)

¹³⁴ Gill, *Capitalism, Communications, and the Corps*, at 111-12 (emphasis added).

conglomerate.”¹³⁵ At bottom, the IRGC’s control over MTN Irancell and TCI was not just about propaganda – the IRGC depended upon such control to support its “security” agenda, i.e., anti-American terror by using the fronts to raise money:

whilst the Guard relied on the communications economy to propagate their ideology, they also ***acquired and monopolised*** communications infrastructure as a ***source of capital gain***. The Guard’s involvement with the communications economy moved beyond the projection of revolutionary ideology, becoming equally a matter of realpolitik and of ***accruing military capital***.¹³⁶

2. Telecommunications Company Of Iran (TCI)

397. In 2009 – four years after the IRGC’s strategy to illicitly source terrorist material through Irancell relied upon “using IEDC as a front” in the IRGC’s 2005 agreement with MTN Group – the IRGC emerged from its previous position of cover on Irancell to publicly assume a majority stake in Iranian telecom company, TCI:

In addition to rejecting foreign majority ownership in Iranian telecommunications infrastructure, IRGC telecommunications activity was driven largely by ‘lucrative no-bid contracts awarded by the Iranian government’. Testament to this, in September 2009, shortly after the violent protests following Ahmadinejad’s re-election, the government announced plans to privatise TCI. Amongst the investors were ***numerous IRGC-backed institutions***, including the IRGC-CF, the Mostazafan Foundation, and the Execution of the Imam’s Order company. Minutes after TCI was privatised, ***the IRGC acquired 51% of the company*** in a \$5 billion deal—the ‘largest trade in the history of the Tehran Stock Exchange’. This represented ***‘yet another calculated step’ in the IRGC’s campaign to dominate Iran’s communications economy***. Rather than using IEDC as a front, as they had done in 2005, the ***IRGC had overtly purchased a majority stake*** in TCI’s monopoly over Iranian telecommunications.¹³⁷

¹³⁵ Gill, *Capitalism, Communications, and the Corps*, at 112.

¹³⁶ Gill, *Capitalism, Communications, and the Corps*, at 112 (emphasis added).

¹³⁷ Gill, *Capitalism, Communications, and the Corps*, at 105-06 (emphasis added).

V. DEFENDANTS FURTHERED THE CONSPIRACY AND TRANSACTED BUSINESS WITH FRONTS, OPERATIVES, AND AGENTS CONTROLLED BY HEZBOLLAH, THE QODS FORCE AND REGULAR IRGC

398. ZTE and Huawei (alongside co-conspirator MTN) did business with fronts, agents, and operatives for Hezbollah, the Qods Force, and Regular IRGC.

399. The IRGC controlled the entire Iranian telecom sector from top to bottom. The following Iranian fronts, operatives, and agents played especially prominent roles in ensuring that any telecom transactions in Iran benefited the IRGC's, including Hezbollah's and the Qods Force's, global terrorist agenda.

A. The Bonyad Mostazafan

400. The Bonyad Mostazafan, also known as the *Bonyad Mostazafan va Janbazan*, Mostazafan Foundation, and Alavi Foundation (herein, the "Bonyad Mostazafan"), was established after the Islamic Revolution to steal and manage property, including that originally belonging to religious minorities in Iran such as Baha'is and Jews, to fund the export of the Iran's Islamic Revolution around the world.

401. The Bonyad Mostazafan was and is an IRGC, including Hezbollah and the Qods Force, front. The Bonyad Mostazafan's purpose was and is to raise funds and obtain weapons (including weapons components) for the IRGC's, including Hezbollah's and the Qods Force's, terrorist operatives and proxies like al-Qaeda and the Taliban. As a front for Hezbollah, the Qods Force, and Regular IRGC funds and weapons (including weapons components) provided to the Bonyad Mostazafan through its commercial transactions inevitably flowed through TCI to Hezbollah and the Qods Force and, through them, to IRGC proxies al-Qaeda and the Taliban, including its Haqqani Network, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

402. At all times, the Bonyad Mostazafan has been led by an agent or cut-out for Hezbollah, the Qods Force, and Regular IRGC and has served as a central hub of IRGC, including Hezbollah and the Qods Force, fund raising, weapons development and acquisition, computing, and communications infrastructure for Iran's terrorist enterprise, which value has flowed through the IRGC to al-Qaeda and the Taliban.¹³⁸

403. The Bonyad Mostazafan is currently led by IRGC Brigadier General Parviz Fattah, who is also, on information and belief, a Qods Force operative.

404. The Bonyad Mostazafan has been widely understood in business, diplomatic, military, and media circles to be a front for Iranian terrorism through Hezbollah, the Qods Force, and Regular IRGC since the 1990s.

405. On May 28, 1995, the Bonyad Mostazafan's status as an Iranian terrorist front made international news when *Newsday* – which was republished around the world through various affiliate relationships – reported that the Bonyad Mostazafan served as a front for raising money and sourcing weapons for Iran's terrorist proxies, including Hezbollah:

[I]n a four-month investigation based on dozens of interviews with law-enforcement officials and U.S. government specialists, knowledgeable Iranians who support the regime as well as dissidents, and public and private documents, *Newsday* has found that:

- [The Bonyad Mostazafan] ... is controlled by Iran's clerical leadership, federal officials say.
- Several of [the Bonyad Mostazafan's] current and former officers and directors have been ***implicated in arms and technology shipments to Iran***, and a former president of the foundation allegedly tried to ship germ-warfare agents to Tehran, according to these officials.

¹³⁸ For example, Mir Hossein Mousavi, who directed the Bonyad Mostazafan for almost a decade, was "the Butcher of Beirut," played a key role in Hezbollah's leadership council and in its attacks on Americans in Lebanon, including the 1983 Marine barracks bombing.

- [The Bonyad Mostazafan] *served as a front* ... for the placement of agents from the [IRGC, including Qods Force], dedicated zealots who ... spy and *obtain military technology* from the United States and abroad.
- [The Bonyad Mostazafan] finances [entities] in the United States that support Iran's militant version of Islam and provides safe haven for groups and individuals supporting the Islamic terrorist group[] ... *Hezbollah*. ...

In a classified report ... the FBI asserted that [the Bonyad Mostazafan] was “entirely controlled by the government of Iran,” which *used [the Bonyad Mostazafan] to set up “covert subbranches disguised* as educational centers, mosques and other centers.” ... The FBI report, according to a U.S. official, claims that [the Bonyad Mostazafan] *funds “fundamentalist extremist groups”* and that Iranian students who received scholarships from [the Bonyad Mostazafan] to study in the United States *“gather[ed] intelligence”* ... and *collected “technical and scientific information” for the Iranian regime*.

In 1989, Oliver Revell, then the No. 2 official at the FBI, told the Senate terrorism subcommittee that some of the “students” receiving [the Bonyad Mostazafan] grants were in fact [IRGC, including Qods Force] agents. ... Revell ... said much of [the Bonyad Mostazafan]’s funds go to “a great number of mosques (in the United States) . . . where there are *organizations which directly support Hezbollah...[,]*” an Iranian-supported militant group ... that has launched terrorist attacks under the tutelage of the Revolutionary Guards. ... *The [Bonyad Mostazafan] is administered by Mohsen Rafiqdoost, founder of the Revolutionary Guards*. Rafiqdoost reports only to the Ayatollah Ali Khamenei, Iran’s spiritual leader.¹³⁹

¹³⁹ Knut Royce and Kevin McCoy, *Militants Build On Iranian Foundation*, Newsday, republished by Pittsburgh Post-Gazette (May 28, 1995), 1995 WLNR 2452536 (emphasis added). After the Islamic Revolution, the Ayatollah seized what had previously been the Alavi Foundation and merged it with the Bonyad Mostazafan. Thereafter, they were one and the same and always were indistinguishable and different names for the same Iranian terrorist front. See, e.g., *id.* (“Vincent Cannistraro, who left the CIA in 1990 as a top official of its counterterrorism center, said in a recent interview, ‘The [Bonyad Mostazafan] and the Alavi Foundation are the same, under different names.’ Other U.S. officials agreed.”).

406. In the same investigative report, *Newsday* also disclosed that “U.S. and European officials say that [the Bonyad Mostazafan] has long been a front for the procurement of military goods and prohibited technology for Iran, particularly for the Revolutionary Guards.”¹⁴⁰

407. The same *Newsday* report also disclosed that “[the Bonyad Mostazafan]’s secretary until 1992, Mojtaba Hesami-Kiche, was at the same time the executive secretary of Vena Industries, a German company wholly owned by [the Bonyad Mostazafan], according to public records filed in Germany. U.S. sources said that Vena has been active in “military procurement” for the Tehran regime.”¹⁴¹

408. Prior to publishing its international media blockbuster report on Bonyad Mostazafan, *Newsday* questioned the Bonyad Mostazafan about its connections to terrorism and allegations that it was used as a front to raise money and source weapons for Iranian terrorist proxies like Hezbollah. The Bonyad Mostazafan replied, through counsel, that it “ha[d] no interest in responding” to such because of their “provocative tone.”¹⁴²

409. When *Newsday* published its investigation revealing that the Bonyad Mostazafan served as a front for providing money, weapons, and logistical support to Hezbollah, the latter was already a U.S.-government designated terrorist group, having been designated by the United States as a Specially Designated Terrorist several months prior. As a result, from 1995 onwards, the Bonyad Mostazafan’s status as a front for Iranian terrorist operations, including the IRGC’s,

¹⁴⁰ Knut Royce and Kevin McCoy, *N.Y. Foundation Linked To Iran’s Islamic Militants*, *Newsday*, republished by Seattle Times (May 26, 1995), 1995 WLNR 1308563 (“Royce and McCoy, *N.Y. Foundation Linked*”).

¹⁴¹ *Id.*

¹⁴² *Id.*

including the Qods Force's, support for Hezbollah was widely known in the international business community and known to Defendants.¹⁴³

410. In 1998, *Newsday* again reported on the western intelligence services' consensus that the Bonyad Mostazafan was a front for funneling funds and weapons to Iranian proxies:

[T]he quasi-official Mostazafan Foundation [] controls billions of dollars of investments in Iran and around the world. The foundation ... ***has been accused by western intelligence services of espionage, supporting terrorism*** and smuggling arms. ... *Newsday* disclosed in 1995 that several officers and directors ... had been implicated in arms and technology shipments to Iran, that it was controlled by Iran's clerical leadership and that the ***FBI believed it had served as a front for placement in the United States of Revolutionary Guards [Qods Force]***, Iranian zealots who conducted espionage and stole military technology.¹⁴⁴

411. After these two *Newsday* reports in 1995 and 1998, the media regularly published similar reports thereafter, which routinely described the Bonyad Mostazafan as a front or funding source for Iranian-backed terrorists operating in the Middle East, including Hezbollah.

412. On December 17, 2008, the U.S. government reinforced its messaging that the Bonyad Mostazafan was a terrorist front that served to raise money and source weapons for Hezbollah, the Qods Force, and Regular IRGC. On that date, the U.S. Departments of Justice, Treasury, and State all announced enforcement actions and sanctions against the Bonyad Mostazafan, and the U.S. Department of State's Counterterrorism Office issued a press release calling attention to U.S. sanctions against entities affiliated with Bonyad Mostazafan.

¹⁴³ For example, the *American Spectator* published an expose in 1995 that revealed multiple Bonyad Mostazafan uses of the U.S. banking system to route funds to terrorist operatives and fronts, and the presence of an IRGC-controlled bank in its New York offices. *See generally* Kenneth R. Timmerman, *Islamic Iran's American Base*, *American Spectator* (Dec. 15, 1995) (discussing the IRGC's use of the Alavi, i.e., the Bonyad Mostazafan, to support terrorist operatives).

¹⁴⁴ Knut Royce, *No Legal Recourse In Iranian's Case / Supreme Court Won't Reopen Suit*, *Newsday* (Dec. 8, 1998), 1998 WLNR 604387 (emphasis added). Since the IRGC personnel placed in the United States through the Mostazafan Foundation were operating overseas, they were Qods Force.

413. The heightened U.S. crackdown on the Bonyad Mostazafan caused a new round of media coverage drawing attention to the Bonyad Mostazafan's status as a front for Iranian terror. For example, the *Washington Post* reported that:

A Fifth Avenue building ... is secretly co-owned by an Iranian bank that helped finance that country's nuclear program, the Justice Department alleged []. Justice is seeking to seize the share of the property ..., charging that 40 percent of [the building] was actually co-owned by Iran's Bank Melli ...[,] [which] was previously designated by the Treasury Department as a key financier of ... the **[IRGC] and the Quds Force, which has been linked to terrorist groups.** ... "This **scheme to use a front company ... to funnel money from the United States to Iran is yet another example of Iran's duplicity,**" said Stuart Levey, the Treasury Department's undersecretary for terrorism and financial intelligence.¹⁴⁵

414. The Bonyad Mostazafan's notorious reputation for directly funding Iranian terrorist proxies in the Middle East continued at all relevant times. For example, in 2014, Jonathan Schanzer, the Vice President of Research at the Foundation for Defense of Democracies, testified that "[t]he Bonyad-e Mostazafan" was "a splinter of Iran's IRGC" and had "reportedly opened its coffers to Hamas, providing critical financial support."¹⁴⁶

415. On November 18, 2020, the U.S. Treasury Department designated the Bonyad Mostazafan, observed that it served as a "bridge to the IRGC," and announced as follows:

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) took action today against a key patronage network for the Supreme Leader of Iran, the Islamic Revolution Mostazafan Foundation (Bonyad Mostazafan, or the Foundation) ... While Bonyad Mostazafan is **ostensibly** a charitable organization charged ..., its holdings are expropriated from the Iranian people and are used by [Ayatollah] Khamenei to ... enrich his office, reward his political allies, and persecute the regime's enemies. ... "Iran's Supreme Leader uses Bonyad Mostazafan to reward his allies under the **pretense of charity,**" said Secretary Steven T. Mnuchin. ...

¹⁴⁵ Glenn Kessler, *U.S. Links Iranian Bank To Fifth Avenue Building*, *Washington Post* (Dec. 18, 2008) (emphases added), 2008 WLNR 28032529.

¹⁴⁶ Statement of Jonathan Schanzer, Vice President of Research at the Foundation for Defense of Democracies, Committee on House Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade. Subcommittee on the Middle East and North Africa, *Hamas and Terrorism*, Congressional Testimony via FDCH (Sept. 9, 2014), 2014 WLNR 24926764.

PARVIZ FATTAH, BONYAD MOSTAZAFAN'S BRIDGE TO THE IRGC

Bonyad Mostazafan maintains close ties to the IRGC, personified by current Foundation president and former IRGC officer **Parviz Fattah**. Appointed to the presidency of the Foundation by the Supreme Leader in July 2019, Fattah previously . . . served as head of the Imam Khomeini Relief Committee, whose Lebanon branch was designated pursuant to *counterterrorism authorities in 2010 for being owned or controlled by, and for providing financial and material support to, Hizballah*. Known for his loyalty to the Supreme Leader, Fattah has also forged ties to senior IRGC-Qods Force (IRGC-QF) officials. According to Fattah, former IRGC-QF commander Qassem Soleimani sought Fattah's assistance to finance the Fatemiyoun Brigade, an IRGC-QF-led militia composed of Afghan migrants and refugees in Iran coerced to fight in Syria under threat of arrest or deportation. . . . The Fatemiyoun Brigade, like the IRGC-QF itself, is designated pursuant to [] counterterrorism . . . authorities. . . .

SANCTIONS IMPLICATIONS

As a result of today's action, . . . OFAC's regulations generally prohibit all dealings by U.S. persons or within (or transiting) the United States that involve any property or interests in property of blocked or designated persons. In addition, persons that engage in certain transactions with the individuals or entities designated today may themselves be exposed to sanctions. . . .¹⁴⁷

416. The Bonyad Mostazafan primarily serves as a front for terror and performs little legitimate charitable work. As the Treasury Department found when it imposed sanctions, “[w]hile the Supreme Leader enriches himself and his allies, the Foundation’s primary mission to care for the poor has *become a secondary objective*. According to the Foundation’s previous president, in past years as little as *seven percent of the Foundation’s profit* has been spent on projects aimed at reducing poverty.”¹⁴⁸

417. The Bonyad Mostazafan directly funds Iranian terrorist proxy military activities outside of Iran. Fattah, who currently runs the Bonyad Mostazafan, has publicly admitted it.

¹⁴⁷ U.S. Treasury Dep’t, *Treasury Targets Vast Supreme Leader Patronage Network and Iran’s Minister of Intelligence* (Nov. 18, 2020) (emphases added).

¹⁴⁸ *Id.* (emphases added).

418. Fattah was separately designated for his terrorism-related connections in 2010.¹⁴⁹

419. The Bonyad Mostazafan's participation in Irancell played a role in persuading the State Department to conclude (as published online) that Irancell was "fully owned by the IRGC."¹⁵⁰

B. Iran Electronics Industries

420. Iran Electronics Industries, also known as IEI, Sanaye Electronic Iran, Sasad Iran Electronics Industries, or Sherkat Sanayeh Electronics Iran ("IEI"), was and is a front for Hezbollah, the Qods Force, and Regular IRGC.

421. IEI's express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of the IRGC's, including the Qods Force's, terrorist operatives and proxies, including Hezbollah. Funds and weapons (including weapons components) obtained by IEI through its commercial transactions inevitably flowed through IEI to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban, including its Haqqani Network, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

422. Since the 1990s, IEI has been widely understood in business, diplomatic, military, and media circles to be a front for Iranian terrorism through Hezbollah, the Qods Force, and Regular IRGC.

¹⁴⁹ U.S. Treasury Dep't, *Fact Sheet: Treasury Designates Iranian Entities Tied to the IRGC and IRISL* (Dec. 21, 2010) ("Parviz Fattah, the Executive Director of Bonyad Taavon Sepah was designated today for acting on behalf of, and providing services to, Bonyad Taavon Sepah.").

¹⁵⁰ U.S. State Dep't Cable, *U/S Levey Seeks Turkish Cooperation Against Iranian Terrorism Finance & Nuclear Proliferation* (Dec. 18, 2006).

423. On or about 2006, a Treasury official, Stuart Levin, told representatives of MTN's competitor, Turkcell, that IEI was "fully owned" by Hezbollah, the Qods Force, and Regular IRGC.

424. On information and belief, Undersecretary Levin communicated to MTN Group that IEI was "fully owned" by the IRGC and that economic interactions with IEI foreseeably aided Iranian proxy terrorist attacks against Americans.

425. On September 17, 2008, the U.S. Treasury Department designated IEI and explained that it builds weapons intended for use against the U.S. military.¹⁵¹

426. IEI's participation in Irancell played a role in persuading the State Department to conclude (as published online) that Irancell was "fully owned by the IRGC."¹⁵²

C. MTN Irancell

427. MTN Irancell is a joint venture between two IRGC, including Hezbollah and the Qods Force, fronts, the Bonyad Mostazafan and IEI, which collectively own 51% of MTN Irancell, and MTN Group Ltd., which owns 49% of MTN Irancell ("MTN Irancell").

428. MTN Irancell was and is a front for Hezbollah, the Qods Force, and Regular IRGC.

429. MTN Irancell's express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of the IRGC's, including Hezbollah's and the Qods Force's, terrorist operatives and proxies like al-Qaeda and the Taliban, including its Haqqani Network. Funds and weapons (including weapons components) obtained by MTN Irancell through its commercial transactions inevitably flowed through MTN Irancell to

¹⁵¹ U.S. Treasury Dep't, *Treasury Designates Iranian Military Firms* (Sept. 17, 2008).

¹⁵² U.S. State Dep't Cable, *U/S Levey Seeks Turkish Cooperation Against Iranian Terrorism Finance & Nuclear Proliferation* (Dec. 18, 2006).

Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban, including its Haqqani Network, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

430. The U.S. State Department purportedly referred to Irancell (as published online) as being “fully owned by the IRGC.”

431. Irancell’s recognized status as being “fully owned by the IRGC” was also widely reported in the media, beginning in 2010 with the initial *WikiLeaks* reporting, and continuing thereafter. For example, in 2012, the news commentator Greta Van Susteren noted on her widely-watched Fox News show: “we’re talking about Iran, which is trying to wipe ... Israel off the map, ... and *this joint venture* with [MTN Irancell], *it was not a mystery*. In fact, the [U]ndersecretary of [the Treasury, Stuart Levin in] 2006 according to [] *WikiLeaks* ... said that the Iran Cell was [] *fully owned by the Iranian Revolutionary Guard* [Corps].”¹⁵³

432. IRGC specialists agree. For example, in 2015, Dr. Emanuele Ottolenghi, of the Foundation for Defense of Democracies, identified “telecommunications” as a “sector where the IRGC [was] bound to reap economic benefits” because “all three mobile operators in Iran” – including MTN Irancell – “are directly or indirectly partners with IRGC-affiliated companies.”¹⁵⁴

D. Telecommunications Company Of Iran (TCI)

433. The Telecommunications Company of Iran (or TCI) was and is a front for Hezbollah, the Qods Force, and Regular IRGC.

¹⁵³ FOX: On the Record, *Interview with Byron York* (August 7, 2012), 2012 WLNR 16563491 (emphasis added).

¹⁵⁴ Statement of Dr. Emanuele Ottolenghi Senior Fellow Foundation for Defense of Democracies, Committee on House Foreign Affairs Subcommittee on Middle East and North Africa, *Iran Nuclear Deal*, Congressional Testimony via FDCH (Sept. 17, 2015), 2015 WLNR 27612447 (“Dr. Ottolenghi Sept. 17, 2015 Testimony”).

434. TCI is the parent company of MTN Irancell's nominal competitor in Iran, MCI.

435. TCI's express purpose was and is to raise funds and obtain weapons (including weapons components) for the benefit of Iran's terrorist operatives and proxies, including Hezbollah.¹⁵⁵ Funds and weapons (including weapons components) obtained by TCI through its commercial transactions inevitably flowed through TCI to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban, including its Haqqani Network, to fund and arm al-Qaeda and Taliban attacks against Americans in Afghanistan from 2007 through the present.

436. TCI is known to be an IRGC, including Hezbollah and the Qods Force, front. The *Economist's* due diligence unit, the *Economist Intelligence Unit*, reported in 2009 that "[t]he question of possible IRGC involvement in the TCI acquisition was raised in subsequent discussion in the Iranian majlis (parliament)," where "[t]he speaker, Ali Larijani, [was] quoted by Aftab-e Yazd, an Iranian newspaper, as saying that the IRGC was a direct party to the deal."¹⁵⁶ The same report also noted the "[b]lurred distinctions" between the IRGC and Iranian telecom companies:

[In 2006,] the Supreme Leader, Ayatollah Ali Khamenei, lent his personal support to the proposed asset sales. As with many other privatisation programmes in authoritarian states, there are strong grounds to suspect that elite groups are manipulating the process to advance their own interests unfairly. It is clear that over the past few years much political and economic power has flowed towards the IRGC. ... The telecoms sector in Iran has expanded rapidly over the past five years, in particular in the mobile segment, which recorded a compound annual growth rate of 65% between 2003 and 2008. There is still room for expansion of mobile telephony as the penetration rate is only about 70%, and broadband services are notably underdeveloped. ***This makes telecoms one of the most attractive targets for investment in Iran.*** At the same time, telecoms is a critical

¹⁵⁵ For example, it was widely reported that, based on purported US diplomatic cables published online, TCI built Hezbollah's secure fiber optic network in Lebanon. See The Guardian, *Lebanon Told Allies of Hezbollah's Secret Network, WikiLeaks Shows* (Dec. 5, 2010), <https://tinyurl.com/2p8by4k3>.

¹⁵⁶ Economist Intelligence Unit, *Iran Telecoms: Dial I for IRGC?*, Telecoms and Technology Forecast (Oct. 12, 2009), 2009 WLNR 20135393.

sector for the security forces, as the Islamic Republic faces unprecedented domestic opposition along with growing external threats. ***If the IRGC is indeed behind the TCI deal, it would make sense from both the commercial and the security perspective.***¹⁵⁷

437. IRGC specialists concur. For example, when Dr. Ottolenghi identified “telecommunications” as “[a]nother sector where the IRGC [was] bound to reap economic benefits,” Ottolenghi also noted that “[t]he IRGC control[led] Iran’s largest telecom company, the Telecommunication Company of Iran or TCI,” which the “[t]he Guards bought ... in September 2009 in a controversial bid that at the last minute disqualified the only non-IRGC offer.”¹⁵⁸ As Dr. Ottolenghi further explained:

TCI’s main shareholder is now Toseye Etemad Mobin (50%), a company ***controlled by the IRGC*** jointly with the supreme leader’s financial network, through two companies - the Tadbir Group-owned Gostaresh Electronic Mobin and Shahriar Mahestan Company. TCI has a monopoly over Iran’s landlines, and thus controls much of the country’s Internet traffic. As *Al-Monitor* reported in August 2013, ***all three mobile operators in Iran are directly or indirectly partners with IRGC-affiliated companies.***¹⁵⁹

E. The Akbari Front Companies

438. Mahmood Akbari, also known as John Wasserman (herein, “Akbari”), was an Iranian resident who purchased dual-use commercial grade computers, related equipment and services from illegal sources in the United States to benefit Hezbollah, the Qods Force, and Regular IRGC. On information and belief, Akbari was an IRGC operative who was used by the Qods Force to serve as a cut-out to help source dual-use technology from America for use by IRGC Syndicate Terrorist Proxies to attack Americans in Afghanistan, doing so upon the instruction of one or more Defendants.

¹⁵⁷ *Id.* (emphasis added).

¹⁵⁸ Dr. Ottolenghi Sept. 17, 2015 Testimony.

¹⁵⁹ *Id.* (emphasis added).

439. Patco Group Ltd. (“Patco”) was a company in the U.A.E. operated by Akbari for the purpose of receiving commercial grade computers and related equipment from illegal sources in the United States to benefit Hezbollah, the Qods Force, and Regular IRGC.

440. Managed Systems and Services (FZC) (“MSAS”) was a company in the U.A.E. operated by Akbari and used as a front company and consignee for computer parts to make it appear that the computer parts were being sent to the U.A.E. when in fact they were being diverted to Iran.

441. TGO General Trading LLC, also known as Three Green Orbit (herein, “TGO”), was a company in the U.A.E. operated by Akbari and used as a front company to make it appear that payments were being made from the U.A.E., rather than from Iran.

442. On information and belief, Patco, MSAS, and TGO (collectively, “Akbari Entities”) were fronts for Hezbollah, the Qods Force, and Regular IRGC that served as cut-outs in order to help Hezbollah, the Qods Force, and Regular IRGC source sensitive dual-use technology from America for the benefit of Iran’s terrorist operatives and proxies, including Hezbollah. Funds and weapons (including weapons components) obtained by the Akbari Entities through their commercial transactions inevitably flowed through Akbari Entities to Hezbollah, the Qods Force, and Regular IRGC, and through them, to IRGC proxies including, among others, al-Qaeda and the Taliban, to fund and arm the Syndicate terrorist attacks against Americans in Afghanistan from 2012 through 2017.

F. Exit40

443. Exit40 was a front for Hezbollah and the Qods Force.

444. Exit40 procured funds and sensitive dual-use technology from America for the benefit of the IRGC’s terrorist enterprise, including the campaigns of IRGC proxies like al-Qaeda and the Taliban.

445. Funds and weapons (including weapons components) obtained by Exit40 through their commercial transactions with Defendants inevitably flowed through Exit40 to Hezbollah and the Qods Force and, through them, to al-Qaeda and the Taliban to fund and arm al-Qaeda's and the Taliban's terrorist attacks against Americans in Afghanistan from 2011 through 2016.

VI. EACH DEFENDANT AND CO-CONSPIRATOR ENGAGED IN COMMERCIAL TRANSACTIONS THAT IT KNEW WERE STRUCTURED TO FINANCE, ARM, AND/OR OPERATIONALLY SUPPORT HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AND THEIR TERRORIST PROXIES IN AFGHANISTAN

A. Co-Conspirator MTN Group

1. MTN Group Entered Its Transnational Corporate Alliance With Hezbollah, The Qods Force, And Regular IRGC In Order To Seize The "Virgin" Telecom Markets In Iran, Afghanistan, Syria, Yemen, And Lebanon, Each Of Which Was Controlled, Contested, Or Influenced By The IRGC And Its Terrorist Proxies

446. The MTN Co-Conspirators consist of two companies that each provided material support to Hezbollah, the Qods Force, the Regular IRGC, and the Taliban, including its Haqqani Network (MTN Group and MTN Dubai) and one company that serves as a front for the IRGC (MTN Irancell). MTN Group and MTN Dubai are MTN Afghanistan's parent companies that held themselves out as responsible for how MTN Group affiliates worldwide manage "security" issues.

447. MTN Group oversaw and authorized MTN Afghanistan's practice of providing support to the Taliban, as well as MTN Group and MTN Dubai's aid routed through MTN Irancell, Exit40, and the other sources of MTN Irancell-related cash-flow alleged in this Complaint.

448. MTN Group executed the Letter Agreement with the Iranian Shareholders on behalf of the entire MTN corporate family. On information and belief, the President of MTN Group was personally compelled to do so during an in-person meeting at the Bonyad Mostazafan

office in Tehran, Iran, when an IRGC Regular Brigadier General communicated to MTN Group's President that the Iranian Shareholders insisted that MTN Group execute the Letter Agreement on behalf of the entire MTN corporate family.

449. On information and belief, the Letter Agreement reflects the Iranian Shareholders' template "Security Aid" agreement, and the Iranian Shareholders specifically styled MTN Group as "MTN" in the Letter Agreement to reinforce to MTN Group and its President, that he was committing the entire MTN corporate family to the deal.

450. It would not be proper to interpret the reference to MTN Group's performance of its "security" related services for the Iranian Shareholders to be limited to being "in South Africa." That passage was a reference by the Iranian Shareholders to their prior frustration with Turkcell, whose C-Suite leadership, on information and belief, refused to commit to providing "security" services to the Iranian Shareholders.

451. MTN Group maintained direct contact with the MTN Afghanistan security official responsible for interfacing with the Taliban, and MTN Group officials encouraged and approved MTN Afghanistan's practice of paying off the Taliban. MTN Group also instructed MTN Afghanistan to comply with the Taliban's directives to switch off its cell towers at night.

452. MTN Dubai was an MTN Group subsidiary and shell company created for financial and tax purposes. It contained no independent business operations from MTN Group, was run by MTN Group employees, and agreed as part of a U.S.-based financing deal to assume responsibility for MTN Afghanistan's operations – including its interactions with the Taliban.

453. MTN Group also furthered the Conspiracy by coordinating strategic communications to provide concealment for the Conspiracy by reaching into the United States to communicate IRGC disinformation concerning whether Irancell is an IRGC front.

454. MTN Group follows a hub-and-spoke business model where the Group headquarters in South Africa provides a substantial amount of financial, operational, technical, and personnel support to every other MTN subsidiary and affiliate.¹⁶⁰

455. MTN Group and MTN Dubai worked closely to coordinate the technical buildout of MTN Irancell, and senior executives from MTN Group and MTN Dubai regularly coordinated their financial, technical, and logistical support to MTN Irancell.

456. Plaintiffs use the term “MTN” in this section to refer collectively to the MTN family of companies. Unless otherwise specified, when Plaintiffs use that term to describe MTN’s conduct in Afghanistan, “MTN” refers to conduct that was implemented on the ground by MTN Afghanistan and approved by both MTN Group and MTN Dubai, and when Plaintiffs use that term to describe MTN’s conduct in Iraq and concerning Irancell, “MTN” refers to conduct that was implemented on the ground by MTN Irancell and approved by both MTN Group and MTN Dubai.

2. MTN Group, MTN Dubai, And All MTN Subsidiaries And Affiliates Worldwide Joined The Terrorist Conspiracy

i. MTN Group Effectively Serves As A Joint Venture Partner With MTN Irancell And Its Iranian Shareholders, The IRGC, Including Its Hezbollah Division And Qods Force

457. MTN Group’s business model depends on MTN Group’s ability to remain well-resourced in order to make significant investments as necessary. This model recognizes that many MTN joint ventures and subsidiaries may have capital expenditure (“CapEx”) challenges

¹⁶⁰ In such a business model, one can ordinarily infer a reasonable estimate regarding the range of monies the hub (here, MTN Group) can be presumed to be reinvesting back into the spoke (here, MTN Irancell), so that the latter can sustainably grow. On information and belief, MTN Group reinvests at least five percent (5%) of MTN Group’s net income derived directly or indirectly from MTN Irancell back into MTN Irancell.

as they scale their business – a classic corporate function where MTN Group can, and ordinarily does, contribute funds and personnel.

458. During the 2010s, MTN Irancell tore through its CapEx. In a business model similar to that of MTN Group, MTN Irancell's CapEx issues were beneficial for MTN Group as it reflected growth and profit. On information and belief, MTN Group provided one or more infusions of cash to MTN Irancell.

459. From 2003 through 2018, MTN Group served in an over-sized role compared to other competitors' parents: Global CEO (recall that MTN Group's CEO committed every MTN entity to the Letter Agreement); Global Logistics and Supply Chain, Global Back-Office;; and Global Financier. Simply put, MTN Group did it all.

460. Beginning in 2004, MTN Group and MTN Dubai pursued an aggressive expansion in the Middle East, in which MTN Group and MTN Dubai worked together to dominate the "virgin" mobile markets of Iran, Afghanistan, Lebanon, Syria, and Yemen.

461. By 2004, few "virgin" market opportunities remained in the world. The collective market share attributed to this Iranian-dominated "Shiite Crescent" of Iran, Syria, and Lebanon, combined with the two other nations where Iran actively fomented terrorist proxies (Afghanistan and Yemen), was by far the most lucrative "virgin" mobile phone market opportunity in the world at the time.

462. MTN Group and MTN Dubai knew that the IRGC, through its subordinate divisions, Hezbollah and the Qods Force, actively sponsored anti-American terrorism in all five of the markets they coveted: Iran, Syria, Lebanon, Afghanistan, and Yemen.

463. Mobile phone companies like MTN Group and MTN Dubai are heavily dependent upon infrastructure vulnerable to terrorist attacks. As a result, MTN Group and MTN

Dubai knew they would have to reach an agreement with the IRGC, which was the only way MTN Group and MTN Dubai could win the business, not just in Iran, but also in its client states (e.g., Syria, Lebanon), or where it played a spoiler role (e.g., Afghanistan). This meant MTN Group and MTN Dubai had to make a deal with the IRGC as the latter exercised a de facto veto over the telecoms' procurement decisions in Syria and Lebanon (among other places).¹⁶¹

ii. On September 18, 2005, MTN Group's CEO And President Caused Every MTN Entity Worldwide To Join the Terrorist Conspiracy When He Executed The IRGC's "Security" Agreement On Behalf Of MTN Group, MTN Dubai, And All MTN Subsidiaries, i.e., "MTN"

464. MTN secured its joint venture with Hezbollah, the Qods Force, and Regular IRGC — i.e., MTN Irancell — through MTN's direct contractual promise to the IRGC, its Hezbollah Division, and Qods Force. This was done in order to aid the IRGC and Qods Force terrorist enterprise and MTN's corrupt payments to one or more IRGC and Qods Force agents.

465. A leaked report from a South African intelligence agency confirmed MTN Group's terrorism quid-pro-quo with the IRGC. One month after the September 2005 in which MTN Group's CEO signed the secret Letter Agreement pledging "security" assistance to the "Iranian shareholders," i.e., the IRGC, which at that time was an Iranian delegation led by the head of Iran's Supreme National Security Council, Hassan Rouhani.

¹⁶¹ MTN Group and MTN Dubai each have deep experience doing business throughout the Middle East. As such, they knew of the widespread, and often reported, practice of the IRGC/IRGC, through Lebanese Hezbollah and the Qods Force, to regularly interfere in the ministerial decisions of its neighbors on commercial, military, and political matters. MTN Group and MTN Dubai therefore knew that all roads to the business in Lebanon, Syria, Afghanistan, and Yemen traveled through the "Iranian Shareholders," i.e., the IRGC, including its Lebanese Hezbollah division and the Qods Force.

iii. After Joining The Conspiracy, MTN Group And MTN Dubai Routinely Acted In Furtherance Of The Conspiracy

466. MTN Group and MTN Dubai joined the conspiracy more than sixteen (16) years ago in 2005, when MTN Group's President and CEO executed the IRGC's terrorist template contract on behalf of all MTN entities worldwide. This committed MTN Group, MTN Dubai, and every other MTN entity to provide "security" assistance to the "Iranian Shareholders," meaning Hezbollah, the Qods Force, and Regular IRGC.

467. MTN Group and MTN Dubai have not exited the conspiracy.

468. MTN Group acted as an international logistics and financial agent for the IRGC, including its Hezbollah Divisions and Qods Force. In doing so, MTN Group acted within the scope of the instruction from MTN Group (the principal) in the Letter Agreement from the "Iranian Shareholders," committing the MTN Group to assist the "security" operations (i.e., terrorist attacks) of Hezbollah and the Qods Force. Indicia of MTN Group's service as an agent for the IRGC include, but are not limited to:

- MTN Group represented the Iranian Shareholders as their purchasing agent, and coordinated efforts to obtain vital U.S. technology that aided bomb and rocket construction and terrorist surveillance, as requested by IRGC-QF and Hezbollah, reaching into U.S. to acquire such gear;
- MTN Group Repeatedly sourced precious U.S. dollars to funnel to IRGC-QF as bribes (\$400,000) or to pay to others as bribes in order to help further conceal IRGC-QF front companies, including pursuing a scheme to bribe the South African UN delegation in order to successfully kill a UN resolution that would have sanctioned IRGC-QF front companies necessary to the terrorist enterprise;
- MTN Group provided public relations support and crisis management services designed to benefit the IRGC-QF front, MTN Irancell, by coordinating the strategic communications response to media stories, government investigations, and/or lawsuits that exposed MTN Irancell as an IRGC-QF front;
- MTN Group Organized IRGC-QF finances and managed IRGC-QF assets through Irancell, and MTN Group had to reach into the United States to do so because of the complicated technology that MTN used, which relied on purloined American technology;

- MTN Group coordinated the secret use of U.S. IT experts to handle sensitive tasks that Irancell personnel could not, knowing that such contractors were performing their work from the U.S. (indeed that was the point, since MTN needed people who had U.S. tech expertise); and
- MTN Group prepared detailed studies at the request of the IRGC-QF that were designed to improve Iranian weapons capabilities, with a specific understanding that the IRGC-QF's primary target was the United States, and therefore that the weapons studies they were sharing would target the U.S.

iv. MTN Group's And MTN Dubai's Recent Conduct Demonstrates That MTN Group And MTN Dubai Remain Active Co-Conspirators With Foreign Terrorist Organizations

469. In 2004, Iran awarded a cellular-phone license to MTN's competitor, Turkcell. MTN then engaged in a corrupt scheme to take the license away from Turkcell and enter the Iranian market itself. MTN's efforts were successful and led it to acquire a 49% stake in Irancell – a joint venture with an Iranian government-controlled consortium. MTN internally called its corrupt scheme to enter the Iranian market "Project Snooker".¹⁶²

470. MTN threw itself into Project Snooker with abandon, dedicating senior MTN Group executives to the mission, including, but not limited to, its President and CEO, Commercial Director, and the regional head responsible for the Middle East.

471. On November 16, 2004, MTN's Commercial Director, Irene Charnley, documented MTN's aggressive support for the terrorist agenda of Hezbollah, the Qods Force, and Regular IRGC. In a fax to Iranians, Ms. Charnley provided MTN's help to Iranian efforts to violate terror-related sanctions against Hezbollah, the Qods Force, and Regular IRGC by sourcing "major components" for American-made "Bell" and "Sikorsky" helicopters that were intended, in part, for "military use" by Hezbollah, the Qods Force, and Regular IRGC.

¹⁶² See Memorandum from Phuthuma Nhleko to Sifiso Dabengwa *et al.*, *Overview & Way Forward – Project Snooker* (Sept. 21, 2005) ("*Project Snooker Mem.*").

472. Project Snooker required close cooperation between MTN and the Iranian government. On July 5, 2005, MTN sent a letter from its CEO to two Iranian terrorists, one of whom was the former Chief of Staff of the IRGC who had led the Bonyad Mostazafan and the IEI, which were the two terrorist fronts with which MTN was attempting to join in the Irancell joint venture (the “July 5, 2005, Letter”). In the July 5, 2005 Letter, MTN Group wrote to its prospective IRGC, including Hezbollah and the Qods Force, joint venture partner:

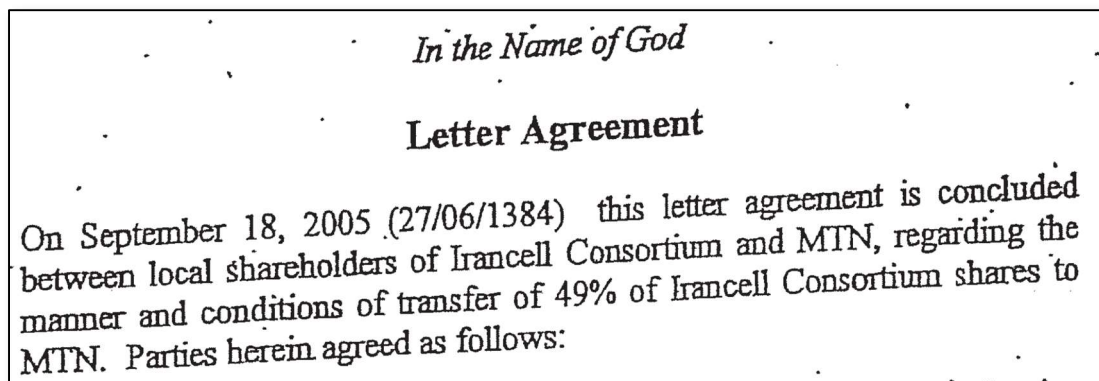
We appreciated the very hospitable manner that you received the MTN Group executive team. During the course of my visit it became clear to me that your organisations play a very important role in the economy of the Islamic Republic of Iran. I was also convinced that your organizations together with MTN could create a partnership that would be *mutually beneficial* in *meeting all our objectives* in the telecommunications sector in Iran.

I would be honoured if you could find the time to pay a visit to the MTN Group Head Office in ... South Africa ... [in] July 2005. ... [D]uring your visit, ... [t]he two key discussion points are:

1. The nature and extent of *financial assistance that the MTN Group could provide to the Iranian partners* in the Second Mobile licence in Iran.
2. The nature and extent of the co-operation between your esteemed organizations and the MTN Group in current and future telecommunications projects in Iran. [Emphases added.]

473. The negotiations were successful. On September 18, 2005, MTN Group signed a Letter Agreement with the IRGC and Qods Force fronts with whom MTN had been negotiating. It gave MTN the right to participate in the MTN Irancell joint venture as a junior partner with a 49% stake, leaving 51% collectively – and all decision-making authority – to MTN’s two partners that MTN knew were IRGC and Qods Force fronts (hereinafter, the “Letter Agreement” or “Agreement”). MTN’s Letter Agreement with Hezbollah, the Qods Force, and Regular IRGC is attached hereto as Exhibit A.

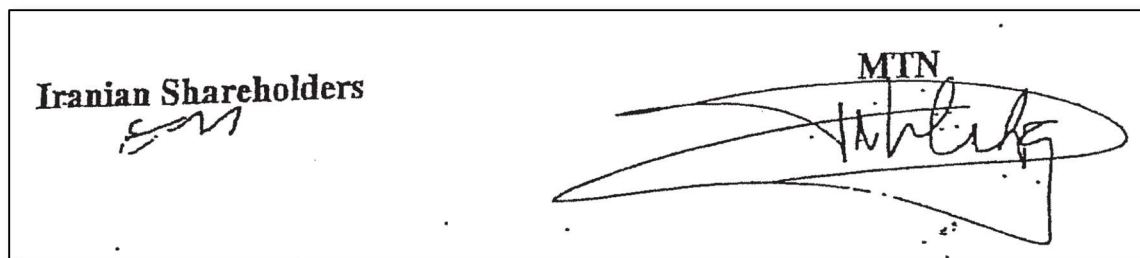
474. The Letter Agreement was drafted by the IRGC and constitutes the IRGC's for the terms under which Iranian terrorist fronts in industries essential to the terrorist enterprise are permitted to enter business arrangements with foreign companies such as Defendants ZTE and Huawei, and co-conspirator MTN. The Letter Agreement is replete with indicia that it was drafted by the IRGC rather than a sophisticated multinational corporation like Defendants. Such indicia include but are not limited to: (1) the reference to God at the start of the Agreement; (2) the inclusion of the Islamic calendar date (27/06/1384) in the Agreement; (3) the generic reference to "Iranian shareholders," rather than any specific reference to any specific Iranian entity; and (4) the inclusion of a blank space for the handwritten insertion of certain terms. Here is how the Agreement begins:



475. The Letter Agreement pledged broad cooperation between MTN Group and its IRGC, including Hezbollah and the Qods Force, partners in furtherance of Iran's terrorist agenda. Section 8 obligated MTN Group to assure that, with respect to its new "Iranian shareholder[]" partners, "[t]he cooperation between MTN and Iranian shareholders should be in the line of defensive, security and political cooperation." Notably, Section 8 expressly contemplated that MTN would work with new IRGC partners outside of Iran: "MTN shall fully support cooperation regarding the aforementioned issues in South Africa."

476. Thus, MTN officers, employees, and agents directly partnered with Qods Force operatives because when MTN “fully” cooperated on “security” matters with IRGC operatives and agents outside of Iran as it contractually promised to do, MTN was directly aiding Qods Force terrorists because IRGC personnel acting outside of Iran are Qods Force.

477. The Letter Agreement’s deliberate ambiguity through its repeated generalized references to “Iranian shareholders,” rather than the Iranian entities with which MTN Group was reportedly partnering, was itself an indication of, and evidence that, the Iranian shareholders in MTN Irancell were fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC. Indeed, the execution of the Agreement was deliberately designed to obscure each signatory:



478. The Letter Agreement did not merely obligate MTN Group to help Hezbollah, the Qods Force, and Regular IRGC source weapons in furtherance of the IRGC’s, including Hezbollah’s and the Qods Force’s, “security” agenda. It also obligated MTN to both pay its new IRGC front partners as well as serve in effect as their financial manager:

- Section 2 required that MTN Group “agreed to put in trust twenty-one (21) percent of Irancell Consortium before Bank Melli as trustee.” Bank Melli is another IRGC, including Hezbollah and the Qods Force, front and has been sanctioned by the U.S. government.
- Section 3 required that MTN pay Hezbollah, the Qods Force, and Regular IRGC hundreds of millions of dollars in up-front license fees as a condition for becoming the new junior partner in the Irancell joint venture, and that “MTN and Bank Melli shall be responsible for arranging project financing.”

- Section 7 set forth an additional catch-all provision designed to route additional money from MTN Group to Hezbollah, the Qods Force, and Regular IRGC and provided that: “[t]he costs and expenses incurred by Iranian shareholders” – i.e., Irancell’s two IRGC, including Hezbollah and the Qods Force, fronts – “if any, due to transfer of Irancell’s share to MTN shall be compensated by MTN.” On information and belief, MTN routed millions of additional dollars to Hezbollah, the Qods Force, and Regular IRGC under Section 7.

479. Although MTN was the IRGC’s junior partner in the MTN Irancell joint venture, the Letter Agreement nonetheless empowered MTN with the legal authorities it needed to effectively shut down the IRGC’s, including Hezbollah’s and the Qods Force’s, ability to weaponize MTN Irancell as an instrument of terror. Most directly, MTN could immediately and unconditionally announce its plans to rapidly exit the joint venture.

480. MTN is also responsible for MTN Irancell’s conduct because MTN had (and continues to have) veto power over most of the major decisions at MTN Irancell, similar to the veto possessed by its joint venture partners, the terrorist fronts Bonyad Mostazafan, and IEI. For example, Section 5.1 of the Agreement provides that:

The resolutions on the below mentioned issues require the affirmative votes of MTN:

- Annual business plans and budgets of [MTN Irancell], including, but not limited to, medium and long term financing;
- Major acquisitions, partnerships, formation of joint ventures or consortiums;
- Discontinuation of business activities;
- Entering into any agreement with persons, individuals or entities that are directly or indirectly related to Non-Iranian or Iranian Shareholders;
- Charging the assets of the Company in any manner which could have significant impact on the Company’s ability to use or benefit from its assets in its ordinary course of business;
- Profit appropriates and dividend policy; and
- Approval of annual accounts.

481. The Letter Agreement confirmed that MTN promised to provide other “off-the-books” value to the Iranian Shareholders with whom MTN had partnered in MTN Irancell, which was itself another obvious reference to MTN’s support for the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist enterprise. Section 9 provides, “for this agreement to be effective, it is necessary that the above-mentioned documents and related agreements be signed by MTN as well as to pay license fee and equity as provided in item 3 above [i.e., Section 3 of the Agreement] within 20 days from the signature of Addendum No. 1 to [sic] license agreement, simultaneously, the parties try to finalize the other relevant operational agreements.”¹⁶³

482. MTN Group and its “Iranian shareholder[.]” joint venture partners went to great lengths to keep the Letter Agreement a secret. The Letter Agreement was a “close hold” document at MTN Group and was only known to a select group of senior MTN Group executives because MTN understood that it memorialized an obviously illegal scheme between MTN Group and two fronts for Hezbollah, the Qods Force, and Regular IRGC. MTN Group also conspicuously failed to obtain any sign-off from any of MTN’s elite, white-shoe global law firms, none of which would have approved the Letter Agreement.

483. Before MTN Group’s President signed the Letter Agreement, a senior official on behalf of the IRGC stated to MTN Group, in sum and substance, that the Letter Agreement was the standard template that the Iranian Shareholders use when a counter-party agrees to assist, among other things, the Iranian Shareholders’ “security” operations.

¹⁶³ In the Letter Agreement, the number “1” in this sentence is handwritten into what was obviously a placeholder.

484. MTN Group, including its President, knew this statement to be a direct reference to IRGC proxy terrorist attacks targeting Americans around the world.

485. MTN Group deliberately concealed the fact that its President and CEO signed the Letter Agreement. On information and belief, MTN Group has never publicly admitted that MTN Group's President and CEO signed the Letter Agreement.

486. MTN Group's attempts to conceal the Letter Agreement, and the fact that MTN Group's President and CEO signed the Letter Agreement, reflects consciousness of MTN Group's guilt and MTN Group's recognition that its promise to assist the Iranian Shareholder's "security" operations, i.e., anti-American terrorism, was illegal.

487. One MTN executive later stated that MTN recognized that it was dealing with a counterparty was comprised of violent killers (referencing the "Iranian Shareholders") whom MTN Group knew ordinarily went around making people mafia-like an "offer they could not refuse," which referred to the negotiating strategy of a violent mafia crime family in the iconic mafia movie, *The Godfather*, in which Don Vito Corleone secured favorable commercial terms that advanced his mafia empire by making a counterparty "an offer he could not refuse," in which he promised to murder the counterparty if he did not give Don Corleone what he desired.¹⁶⁴ On information and belief, officers, managers, employees, and agents of MTN Group and MTN Dubai regularly expressed similar sentiments.

488. MTN Group's executives quickly got to work after MTN Group executed the Letter Agreement on September 18, 2005. Three days later, MTN's President and CEO, Mr. Nhleko, circulated a memorandum from himself to five senior MTN executives (the "September

¹⁶⁴ In the movie, a recalcitrant counterparty refuses to sign a contract demanded by Don Corleone, who dispatches his muscle to communicate to the counterparty that "either his brains or his signature" will be on the contract, which causes the contract to be executed.

18, 2005 Memo”). Captioned “**STRICTLY CONFIDENTIAL**” and headed with the subject “**OVERVIEW AND WAY FORWARD – PROJECT SNOOKER**,” the September 18, 2005

Memo provided, in part, as follows:

1. OPPORTUNITY

Project Snooker still presents *one of the most significant “virgin” mobile opportunities in the world*. ... [N]otwithstanding the significant challenges that lie ahead, [MTN] must continue to pursue this opportunity vigorously.

2. CURRENT STATUS

The signing of the various agreements this week [under duress] was to “book our place at the foot of the mountain – we still need to scale it to get to the peak.” It was a choice between inheriting an advanced arrangement [Turkcell revenue share and various negotiated agreements] or taking the chance that the window of opportunity may close on us whilst we try to reconstruct the deal and arrangements from scratch. We chose the former.

3. RISK AND REWARD

Snooker is “no normal country”. The Ministry of Defense, Government controlled banks and companies, together with Government *essentially control all the commercial activity in the country*. *Consequently, a conventional mindset, orthodox financial and operational approach to this project is unlikely* to provide us with an outcome that I would feel comfortable to recommend to the board on an investment of over €400 million [license fee and working capital] into Snooker. It is therefore imperative to *think laterally on how we can secure the investment* ... in a manner that allows us to penetrate the market achieving an acceptable IRR [i.e., “internal rate of return,” a measure of investment profitability]. ...

4. TIMING

The expectation is that the license fee should be paid within weeks and the operation launched commercially within a six month period. ... The implied time scale can only be achieved through a well thought out and coordinated project management structure up ...

5. PROJECT MANAGEMENT

Given the size of the market, limited time to launch and all that has to be reviewed and completed before the MTN Group board ratifies the revised business plan, *a special project structure must be put in place*. ...

5.1.2 Finance Structure, project funding and ancillary loan agreements

The Group CFO should take responsibility for this area, primarily in the following categories:

- Flow of license fee and working capital
- Appropriate security arrangements for funding of local partners together with the loan agreements
- Arranging the project finance ...

6. PROJECT STEERING COMMITTEE [sic]

I will chair a project steering committee that will have the responsibility of meeting regularly to oversee both Phase I and Phase II until the project is passed onto the MD / COO. The Steering Committee shall comprise of:

CEO

COO

CFO

CTO

Commercial Director

Group Executive HR ...

8. CONCLUSION

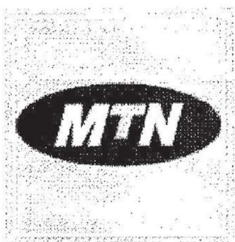
This is one of the most significant opportunities the Group will undertake and will require teamwork to achieve these objectives. [Emphases added; formatting adjusted.]

489. After MTN's executive team successfully executed Project Snooker, the conservative-dominated and Qods Force-applauding Iranian parliament determined that MTN's operation of Irancell would improve Iran's "security."

490. Project Snooker was successful not only because MTN pledged strategic cooperation with the Iranian government, but also because MTN made corrupt payments to government officials, at least one of which it structured as a sham consultancy payment. On December 11, 2006, MTN Group's CEO instructed MTN Group's CFO to "finalise all agreements with the consultants" who had "assisted the Company" in obtaining the Iran deal. The first agreement called for MTN Group to make a \$400,000 payment for the benefit of an Iranian government operative. The payment was effectuated through an MTN Group subsidiary, MTN International (Mauritius) Limited, and sent to a consulting firm owned by the Iranian operative's associate. On April 4, 2007, MTN wired the \$400,000 to the putative "consultant." MTN has never proffered a legitimate explanation for that payment.

491. MTN's second corrupt payment was to South Africa's ambassador to Iran. MTN's Iran Director has admitted to paying the Ambassador \$200,000 in cash out of his own funds, which he tied to cooperation in helping MTN secure its equity interest in Irancell.

492. MTN Group's senior executives knew of, and approved, MTN Group's bribes to Hezbollah, the Qods Force, and Regular IRGC agents who helped MTN secure the Irancell joint venture. For example, on December 11, 2006, MTN's President and CEO, Mr. Nhleko, wrote a memorandum to MTN Group's commercial director, in which Mr. Nhleko authorized MTN's bribes (the "December 11, 2006 Memo"), which provided, in full, as follows:



MEMORANDUM

TO : IRENE CHARNLEY
DATE : 11 DECEMBER 2006
FROM : PHUTHUMA NHLEKO
SUBJECT : CONSULTANCY AGREEMENTS

Dear Irene

With reference to the process in terms of which MTN International (Mauritius) Limited acquired a 49% equity interest in Irancell, you are authorized to finalise all agreements with the consultants that assisted the Company during the run up to and actual negotiating period, and to effect the necessary payments.

Kind regards

A handwritten signature in black ink, appearing to read "Phleko", is written over a horizontal line.

PHUTHUMA F. NHLEKO
GROUP PRESIDENT & CEO

493. The phrase “necessary payments” in the December 11, 2006 Memo was a direct admission that the consultancy payments were bribes. Indeed “necessary payments” has long been understood to refer to bribery.

494. A host of other highly confidential internal MTN Group documents, leaked by a whistleblower, also confirm that MTN Group’s executives directed MTN’s financial, technological, and operational support for MTN Irancell and the IRGC, including Qods Force, fronts that controlled Irancell. For example, a March 25, 2007 memorandum from MTN’s regional manager responsible for Iran, Chris Kilowan, and MTN’s CEO, Mr. Nhleko extensively documents MTN Group’s illicit activities (the “March 25, 2007 Memo”).

495. The March 25, 2007 Memo was intended to remain highly confidential, as reflected by what is set forth at the top of it:

MTN GROUP LIMITED

**MEMORANDUM – HIGHLY
CONFIDENTIAL**



To: Phuthuma Nhleko

From: Chris Kilowan

Date: 25 March 2007

Re: Ambassador Briefing: Larijani, Mottaki and MTN

496. In the March 25, 2007 Memo, MTN’s regional director responsible for Iran confirmed to MTN’s President and CEO that “it was the [President of South Africa’s] view that the matter of MTN has nothing to do with the Government of South Africa as it is a private business in which the Government of South Africa plays no role.”

497. In the March 25, 2007 Memo, MTN’s regional director responsible for Iran confirmed to MTN’s President and CEO that he had met with “Mr. Motakki” on behalf of the “Minister of Foreign Affairs.” On information and belief, “Mr. Motakki” was an IRGC,

including Qods Force, cut-out who was either relaying a message from the IRGC or acting as an IRGC operative himself. In the Memo, MTN's regional director for Iran told its CEO that Mr. Motakki "re-iterated [the IRGC's, including the Qods Force's] understanding that MTN was allowed to replace Turkcell in exchange for defence co-operation," and that "the office of the Supreme Leader" had personally intervened based upon the conclusion by Hezbollah, the Qods Force, and Regular IRGC "that there are significant defence benefits in it for [Hezbollah, the Qods Force, and Regular IRGC] were MTN to be allowed into the process. On that basis [Hezbollah, the Qods Force, and Regular IRGC] withdrew their objections [to a foreign company playing a role in the Iranian telecom sector] and allowed the process to proceed in MTN's favour."

498. In the March 25, 2007 Memo, MTN's regional director responsible for Iran confirmed to MTN's President and CEO that MTN had only become a candidate for the Irancell joint venture after it had promised to pledge to aggressively support the "security" needs of Hezbollah, the Qods Force, and Regular IRGC fronts that controlled the Bonyad Mostazafan and IEI. He noted, as a "brief recap of history," that "MTN only seriously got back into the [bidding] process" after its Iranian counterparties perceived that MTN would affirmatively aid their "security" needs.

499. In the March 25, 2007 Memo (emphases added), MTN's regional director for Iran underscored to MTN's President and CEO that MTN would need to serve as a weapons supplier for its Iranian counterparties if it wanted to win and maintain its position in the joint venture:

It would seem clear that the issue of *defence co-operation* has become a pressing matter with the government of Iran.

If regard is had to the latest UNSC [i.e., U.N. Security Council] Resolution there is a clear move towards dealing with Iran's conventional weapons capability. ... Russia has traditionally played the *role of key weapons supplier* to Iran. Given

recent developments ..., [Russia] is actively looking at more secured suppliers of defence materials. ... Because the entire political situation has now deteriorated significantly it is highly unlikely that the Government of South Africa will be prepared to sign any defence agreements or deliver defence materials to Iran.

Given the *clear linkage that the Government of Iran has drawn between the defence assistance and allowing MTN into the country the likelihood that there will be serious blowback for MTN is increasing.*

Because there has been a recognition of the *non-business imperatives that drove MTN's entry into Iran*, the Distant Thunder ... projects have been developed to deepen MTN's position, as opposed to and distinct from Irancell, inside Iran so that MTN would be able to rely on broad popular support for its continued presence. More recently a more mid to long range strategy has been proposed to ensure that MTN puts in place an exit strategy that would ensure that it not be caught in a situation where it loses its entire investment in the country. ...

I am preparing a document that spell out the range of actions that can be taken against MTN and will submit that to you as soon as it is complete. In summarized form it can be said that there is every possibility that MTN could be effectively isolated from Irancell with very little negative effect on Irancell.

While 1 million subscribers will act as a defensive buffer for Irancell, it does not provide the same protection for MTN. This is because these subscribers are reflected locally as Irancell subscribers and not MTN. *All the innovations are not sold as MTN innovations but as Irancell's.* ...

To give MTN a realistic chance to navigate through what is potentially going to be a difficult few months (if not years until the end of the current presidency in 2009), I make the following recommendations:

1. Implementation of Project Distant Thunder at the earliest opportunity. We could pre-empt some of the activity that is almost certain to be started in the public sphere against MTN. ... (Dimension 1)
2. Approval of the creation of the committee to pursue mid to long term strategies for MTN's investment in Iran. (Dimension 2)
3. Finalisation of the diplomatic support initiative. The *first consultant is still waiting for the transfer of the agreed amount. This is causing considerable anxiety in his mind and going forward we are going to need his support.* We still have not given the second consultant any indication whether we are seriously considering his request. He too is developing some anxiety and I have to field almost daily questions on it. (Dimension 3)

500. A November 10, 2007 memorandum from MTN's regional manager responsible for Iran, Chris Kilowan, and MTN's then-CEO, Mr. Nhleko, further documented MTN Group's open support for the illicit activities conducted by the fronts operating on behalf of Hezbollah, the Qods Force, and Regular IRGC with whom MTN had partnered in Irancell, including MTN partners whom MTN nicknamed "Short John" and "Long John" (the "November 10, 2007 Memo"). On information and belief, the Iranian operative whom MTN derisively nicknamed "Short John" was an agent for Hezbollah, the Qods Force, and Regular IRGC.

501. The November 10, 2007 Memo was labeled "**STRICTLY CONFIDENTIAL**" in bright red bolded all-caps font and was titled "**SUBJECT: OUTSTANDING ISSUES**" in bolded all-caps black font. In it, MTN's executive for Iran communicated to MTN's CEO that:

Pursuant to [our] last communication ... I set out below the issues that I believe are still outstanding [] and will have an impact ... on MTN's investment. ...

2. FINALISATION OF CONTRACT WITH SHORT JOHN

Subsequent to our last discussion on this matter [in early 2007] I did not do anything about the agreement, preferring to wait until December [2007] to do an agreement ... I can certainly state that [Short John] has *come to the party on every occasion that I called upon him*. The fact that the *quid pro quo that has threatened at one stage to be the primary stick with which we could be hit has now largely disappeared* because of his efforts.

The initial concessions on promised support for the revenue share issue was *because of his direct involvement* ... With me out of the picture he will probably be the only friendly source of information and interaction for MTN on this side. I would recommend that *MTN finalise arrangements with him and offer fair compensation commensurate with the huge role he has played right from the outset*.

3. RENEWED APPROACH BY LONG JOHN

I have communicated this to you a few weeks ago and recently forwarded an SMS from him. The background to this new approach is centered in planned developments within the area that he is currently working. Whatever his motivations, it is not something that should be ignored. While he has very

little power to do anything positive, *he can be a destructive force* or simply an unnecessary distraction. ...

6. PERSISTENT NEGATIVE VIEWS ABOUT SOME MTN EXPATS

I beg your forgiveness if I sound like a record with a stuck needle but I ... alert[] you to a serious risk to MTN's investment. ... In [Mr. Mokhber's] view MTN made a mistake and inflicted a huge insult on Iran by placing [a woman] here [as Chief Operating Officer of MTN Irancell]. ...

(Bolded all-caps emphases in original; bolded italicized emphases added.)

502. In June 2018, South Africa's anti-corruption police – called the “Hawks” – raided the offices of MTN and its outside counsel as part of an investigation into Irancell-connected bribery. Roughly eight months later, the Hawks also arrested the former Ambassador whom MTN had bribed. On information and belief, that investigation remains ongoing.

503. One reason MTN chose to become the IRGC's, including Hezbollah's and the Qods Force's, joint venture partner was the potential for enormous profits. As the *Financial Times* reported at the time in 2013, “[a]s the international community was weighing whether to impose yet more sanctions on Iran over its nuclear programme, [MTN President and CEO] Phuthuma Nhleko was making other plans. Instead of seeing a country with mounting political problems, Mr Nhleko saw a nation with relatively few mobile phone users. Iran, he reckoned, could quickly add 2.5m-3m new customers for MTN Group, the mobile phone company he was running in 2006.”¹⁶⁵

504. After MTN secured its joint venture with two fronts for the IRGC, MTN's President and CEO, Phuthuma Nhleko, “laughed off questions about the political risk of doing

¹⁶⁵ Lina Saigol and Andrew England, *Telecoms: Dealings in the Danger Zone; MTN of South Africa's Ventures in Iran and Syria Have Dented Its Reputation and Rattled Shareholders*, *Financial Times* (July 2, 2013) (“Saigol and England, *Telecoms: Dealings in the Danger Zone*”).

business with Iran.”¹⁶⁶ As he chuckled in a discussion with investors after closing the deal with the Iranians, he stated “[MTN] hadn’t budgeted for bomb shelters or anything like that.”¹⁶⁷ MTN’s CEO’s choice to literally “laugh off” questions about the obviously dire risks associated with MTN’s new joint venture in Iran typifies MTN’s deliberate choice to align itself with anti-American terrorists as the cost of doing business as the IRGC’s junior partner in the MTN Irancell joint venture.

505. MTN continued to pursue Project Snooker even after the U.S. Undersecretary of the Treasury told Turkish officials that Irancell was “fully owned” by Hezbollah, the Qods Force, and Regular IRGC. Undersecretary Levey did so as part of a campaign in which he alerted every major western business and financial partner of Hezbollah, the Qods Force, and Regular IRGC about the inherent terrorism risks attendant to any transactions with fronts for Hezbollah, the Qods Force, and Regular IRGC. On information and belief, Undersecretary Levey told MTN Group that Irancell was “fully owned” by Hezbollah, the Qods Force, and Regular IRGC and, by extension, when Irancell operated outside of Iran, Qods Force operatives were in charge.

506. MTN’s bribes and alliance with Hezbollah, the Qods Force, and Regular IRGC “is a saga that illustrates the extraordinary risks MTN has taken to profit from doing business with pariah states.”¹⁶⁸

¹⁶⁶ *Id.*

¹⁶⁷ *Id.*

¹⁶⁸ *Id.*

3. MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC's, Including Hezbollah's And The Qods Force's, Terrorist Enterprise Against Americans Worldwide

507. For more than fifteen years, MTN Group and MTN Dubai has served as a reliable joint venture partner for the world's worst terrorist organization, Hezbollah, the Qods Force, and Regular IRGC.

508. MTN Group coordinated with MTN Dubai to manage the procurement scheme. On information and belief, MTN Group directed the conduct of the purported "third parties" in the U.A.E. who were, in fact, shared corporate covers acting on behalf of both MTN Group, MTN Irancell, and Hezbollah, the Qods Force, and Regular IRGC.

509. MTN Group specifically decided that MTN Group and MTN Dubai would closely coordinate to extract vast amounts of state-of-the-art American technologies from the U.S. marketplace on behalf of MTN Group's IRGC partners. In its Special Report, *Reuters* explained, "[a]ccording to a person familiar with the matter, ***MTN [Group] was determined that MTN Irancell procure substantial amounts of U.S. equipment: The U.S. products had performed well in its other networks, and the company's technicians were familiar with them.***"¹⁶⁹

510. MTN Group, and its employees, set out to evade America's IRGC-related terrorism sanctions. According to *Reuters*, "internal [MTN Group] documents" "show that MTN [Group] employees created presentations for meetings and wrote reports that openly discussed circumventing U.S. sanctions to source American tech equipment for MTN Irancell."¹⁷⁰

¹⁶⁹ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, *Reuters* (Aug. 30, 2012).

¹⁷⁰ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, *Reuters* (Aug. 30, 2012).

511. MTN Group’s employees understood that their transaction activities on behalf of the IRGC were illegal. According to Reuters, “internal [MTN Group] documents” “show that MTN [Group] employees” “address[ed] the potential consequences of getting caught” in written MTN Group documents.¹⁷¹

512. MTN Group’s C-Suite directed its support for the conspiracy, and continued doing so even after MTN Group finished pilfering the Irancell license from Turkcell in 2005:

The new MTN documents appear to detail an *intentional effort to evade sanctions*. For example, a January 2006 PowerPoint presentation prepared for the project steering committee - *comprised of then top-level MTN executives* - includes a slide titled “Measures adopted to comply with/bypass US embargoes.” It discussed how the company had decided to outsource Irancell’s data centre after receiving legal advice. “In the absence of applicable U.S. consents, it is a less risky route to MTN for Irancell to outsource data centre than it is to purchase restricted products,” the PowerPoint slide says.¹⁷²

513. MTN Group, its executives, and employees, knew there were potential “civil and criminal consequences” to their scheme – and intensified it anyway:

“CIVIL AND CRIMINAL CONSEQUENCES”

According to [] internal procurement documents, right from the start MTN was well aware of what it termed “embargo issues” and the *inherent risks involved*. A December 2005 PowerPoint presentation marked confidential and emblazoned with MTN’s logo noted that the *“Consequences of non compliance” included “Civil and criminal consequences.”* The PowerPoint slide added that the U.S. government could blacklist MTN, “which could result in all MTN operations being precluded from sourcing products/services from U.S. based companies.”¹⁷³

514. MTN Group, its C-Suite, and its employees had actual knowledge of the scheme. MTN Group personnel routinely prepared written materials that memorialized the illicit

¹⁷¹ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, Reuters (Aug. 30, 2012).

¹⁷² Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, Reuters (Aug. 30, 2012).

¹⁷³ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, Reuters (Aug. 30, 2012).

importation of embargoed U.S. technologies, for the specific purpose of flowing the technology through to Iran, where MTN Group and its personnel knew there would be only one end recipient: Hezbollah, the Qods Force, and Regular IRGC. Per *Reuters*:

A delivery schedule also dated June 2006 lists U.S. equipment needed for “value-added services,” including voice mail and a wiretapping system. The schedule states that the equipment would be “Ready to Ship Dubai” that July and August. It estimates it would take two weeks to arrive in the southern Iranian port of Bandar Abbas by “Air or Sea/Road,” and then up to 30 days to clear Iranian customs. According to a person familiar with the matter, the equipment ultimately arrived by boat. “It all showed up,” this person said.¹⁷⁴

515. MTN Group maintained “a lengthy spreadsheet of ‘3rd Party’ equipment dated June 2006 that list[ed] hundreds of U.S. components - including servers, routers, storage devices and software - required for a variety of systems.”¹⁷⁵

516. MTN Group, and its employees, set out to evade America’s IRGC-related terrorism sanctions. According to *Reuters*, “internal [MTN Group] documents” “show that MTN [Group] employees created presentations for meetings and wrote reports that openly discussed circumventing U.S. sanctions to source American tech equipment for MTN Irancell.”

517. From the course of negotiations with its IRGC, including Qods Force, counterparts in 2004 and 2005, MTN knew at all times that it was acting to benefit the IRGC’s, including Hezbollah’s and the Qods Force’s terrorist agenda. MTN contractually agreed to benefit the “security” needs of its Iranian Shareholders (a direct reference to the two fronts for Hezbollah, the Qods Force, and Regular IRGC with whom MTN agreed to serve as the junior

¹⁷⁴ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, *Reuters* (Aug. 30, 2012).

¹⁷⁵ Steve Stecklow, *Special Report: Documents Detail How MTN Funneled U.S. Technology to Iran*, *Reuters* (Aug. 30, 2012).

partner in their shared joint venture). MTN's agreement with Hezbollah, the Qods Force, and Regular IRGC is attached hereto as Exhibit A.

518. MTN Group and MTN Dubai knew that MTN's pledge to aid the IRGC's, including Hezbollah's and the Qods Force's, "security"-related efforts committed MTN Group and MTN Dubai to actively participating in the IRGC's, including Hezbollah's the Qods Force's, terrorist enterprise against Americans outside of Iran, including in Afghanistan and Iraq.

519. MTN Group remained committed to its IRGC, including Hezbollah and the Qods Force, allies even after withering U.S. pressure. For example, in or around 2010 or 2011, MTN representatives met with senior executive officials from the U.S. government. During these meetings, MTN representatives falsely assured the U.S. government that they were not helping Hezbollah, the Qods Force, and Regular IRGC or supplying them with any embargoed U.S. technology in violation of U.S. sanctions against Iran that are intended to deprive Hezbollah, the Qods Force, and Regular IRGC of the money and technology useful to their propagation of violence against Americans in Afghanistan and Iraq. MTN provided the U.S. such false assurances even after "MTN ha[d] carried out orders from the regime to shut off text messaging and Skype during times of political protest, and reportedly ha[d] a floor in its Tehran headquarters controlled by Iranian security officials."

520. As the Hezbollah, Qods Force, and Regular IRGC joint venture partner responsible for sourcing the most important technological items for modern terrorism – the communications, computing, and encryption technologies that were vital to attacking Americans – MTN assumed a key financial and operational role in the IRGC's, terrorist enterprise, including their technological support of Hezbollah and the Qods Force.

521. Under the structure of the MTN Irancell joint venture, the two fronts for Hezbollah, the Qods Force, and Regular IRGC that exercised 51% control of MTN Irancell – the Bonyad Mostazafan and IEI – had the mandate to promote the IRGC’s, including Hezbollah’s and the Qods Force’s, “security” agenda, including the obligation to block any significant MTN Irancell-related transaction or commercial relationship unless it improved the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorism capabilities. Given the IRGC’s, including the Qods Force’s, view that MTN Irancell was essential to IRGC, including Hezbollah and the Qods Force, “security” operations, the terrorist fronts that controlled MTN Irancell (Bonyad Mostazafan and IEI) would not have approved any material MTN Irancell transaction unless they determined that, on balance, the particular transaction improved the IRGC’s, including Hezbollah’s and the Qods Force’s, ability to execute terror operations as the central element of the IRGC’s “security” agenda. As a result, one may infer that every significant commercial transaction and business relationship that MTN Irancell entered into was: (1) vetted by Hezbollah, the Qods Force, and Regular IRGC; and (2) determined by such terrorists to advance the IRGC’s, including Hezbollah’s and the Qods Force’s, “security”-related capabilities, which was a specific Iranian euphemism for external terror operations.

522. MTN was the lead target of a major public pressure campaign demanding that MTN exit its joint venture with Hezbollah, the Qods Force, and Regular IRGC. For example, on March 7, 2012, UANI “renewed its call on investors, affiliated institutions and potential customers to cease all business with South African telecommunications firm MTN in response to MTN Group President and CEO Sifiso Dabengwa’s callous remarks and irresponsible posture on MTN’s partnership with sanctioned Iranian entities that are linked to the Islamic Revolutionary

Guards Corps (IRGC).”¹⁷⁶ MTN chose to stay in their alliance with Hezbollah, the Qods Force, and Regular IRGC in the face of such pressure and even after nearly every other multinational had exited such ventures.

523. From 2005 through the present, MTN’s joint venture with MTN Irancell, and MTN’s illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI, the Akbari Fronts, and Exit40 each provided tens of millions of dollars annually in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC, which flowed through to al-Qaeda and the Taliban, including its Haqqani Network and facilitated attacks against Americans in Afghanistan, including Plaintiffs and their loved ones.

i. MTN Assumed A Financial Role In The Terrorist Enterprise

524. MTN assumed a financial role in the terrorist enterprise by, among other things, bribing its IRGC, including Qods Force, joint venture partners to win the Irancell license in the first instance, paying large license fees, and generating revenue for MTN Irancell throughout the operation of the joint venture.

525. “In Iran, MTN has been accused of paying bribes to South African and Iranian officials to secure a licence there in 2005.”¹⁷⁷

a. MTN’s Bribes to Terrorist Fronts

526. On information and belief, the recipient of MTN’s \$400,000 wire acted as a front, operative, or agent for Hezbollah, the Qods Force, and Regular IRGC. On information and

¹⁷⁶ United Against Nuclear Iran (“UANI”), *UANI Responds to MTN CEO’s Irresponsible Position on Iran and Renews Call for MTN to End its Business in Iran* (Mar. 7, 2012); see Business Wire, *UANI Responds to MTN CEO’s Irresponsible Position on Iran and Renews Call for MTN to End its Business in Iran* (Mar. 7, 2012) (broad international publication of this UANI press release).

¹⁷⁷ Agence France Presse English Wire, *South African Telecom MTN Gains Clients Despite Scandals* (Mar. 7, 2019).

belief, the recipient of MTN's \$400,000 wire was a cut-out for MTN to route value to "Iranian shareholders" who were Hezbollah, the Qods Force, and Regular IRGC. Hezbollah, the Qods Force, and Regular IRGC ensures that all economic value is shared amongst constituent parts of the organization, and would not have permitted such value transfer here relating to a contract decision-making process Hezbollah, the Qods Force, and Regular IRGC controlled without obtaining their share of the payment under the IRGC's mafia-like revenue sharing practices.

527. MTN knew, or recklessly disregarded, that the recipient of MTN's \$400,000 wire was acting as a cut-out to allow money to flow through for the benefit of Hezbollah, the Qods Force, and Regular IRGC, which had proved vital to MTN's successful campaign to steal Turkcell's license.

528. MTN also knew, or recklessly disregarded, that the recipient of MTN's \$400,000 wire instructed MTN to wire the money, in U.S. Dollars, to a bank account in the U.A.E., and therefore that the recipient of MTN's \$400,000 wire was specifically acting as a pass-through for the benefit of the Qods Force because MTN's \$400,000 wire instruction, on information and belief, caused a bank in the United States to send \$400,000 to a bank account controlled by a cut-out for Hezbollah, the Qods Force, and Regular IRGC acting in Dubai, which was the Qods Force's most notorious financial and logistical hub in the Middle East outside of Iran.

529. On information and belief, MTN regularly makes similar sham "consulting" payments like one that MTN used to attempt to justify MTN's \$400,000 wire. Such payments benefitted fronts, operatives, or agents for Hezbollah, the Qods Force, and Regular IRGC in their MTN Irancell-related terrorist fundraising efforts from 2005 through today.

b. MTN's License Fee Payments to Terrorist Fronts

530. After it corruptly secured the 15-year Irancell license, MTN Group Ltd. paid Hezbollah, the Qods Force, and Regular IRGC through the Bonyad Mostazafan and IEI, an

approximately \$300 million license fee when it secured its 49% status as the junior partner in the MTN Irancell joint venture. This money benefited the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise, and Hezbollah and the Qods Force received a substantial amount per standard practice by the IRGC.

c. MTN's Funding of Terrorist Fronts through MTN Irancell Cash Flow

531. MTN reaped enormous profits from its involvement in MTN Irancell, and sourced copious amounts of dual-use technology to benefit MTN Irancell and Hezbollah, the Qods Force, and Regular IRGC. Indeed, by 2013, "MTN has faced a huge headache in seeking to get dividends out of Iran because stringent sanctions prevent[ed] banks from moving cash easily in and out of the country. MTN ... *was virtually printing money in Iran*, where it has a 46% share of the market."¹⁷⁸

532. Under MTN's joint venture with its two IRGC, including Hezbollah and the Qods Force, front partners in MTN Irancell, for every dollar (or Iranian Rial) MTN generated for the joint venture, MTN's terrorist partners received 51 cents to invest in their terrorist enterprise. Thus, every dollar in profit for MTN Irancell inevitably helped fund Hezbollah's coordination of a nationwide insurgency against Americans in Afghanistan, the IRGC's, including the Qods Force's, industrial-scale production of IED components, advanced rockets, and other high-tech weapons for use by Syndicate terrorists against Americans in Afghanistan led by al-Qaeda and the Taliban, and the aggressive forward deployment of Hezbollah and/or Qods Force operatives inside Afghanistan to facilitate the IRGC's vast storehouse of assistance to the Taliban.

¹⁷⁸ Business Day Live, *Iran Deals Forced MTN Boss to Quit* (July 28, 2013) (emphasis added).

533. Through its participation in MTN Irancell, MTN caused Hezbollah, the Qods Force, and Regular IRGC to realize tens of millions of dollars per year in income that Hezbollah, the Qods Force, and Regular IRGC used to fund terrorist operations against Americans in Afghanistan including, among other things, by funding al-Qaeda and the Taliban, including its Haqqani Network.

ii. MTN Assumed An Operational Role In The Terrorist Enterprise

534. MTN Group and MTN Dubai deliberately provided “security” assistance to its JV partners, the “Iranian Shareholders,” i.e., Hezbollah, the Qods Force, and Regular IRGC. In its blockbuster Special Report breaking one MTN Group scandal, *Reuters* revealed that “internal documents seen by *Reuters*,” showed that “MTN Group” “*plotted to procure embargoed U.S. technology products for an Iranian subsidiary through outside vendors* to circumvent American sanctions on the Islamic Republic.”¹⁷⁹

535. According to Reuters, “[h]undreds of pages of internal documents reviewed by Reuters show that MTN employees created presentations for meetings and wrote reports that openly discussed circumventing U.S. sanctions to source American tech equipment for MTN Irancell. ... [and] also address[ed] the potential consequences of getting caught.”¹⁸⁰ Indeed, “[t]he documents show that MTN was well aware of the U.S. sanctions, wrestled with how to

¹⁷⁹ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

¹⁸⁰ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

deal with them and ultimately decided to circumvent them by relying on Middle Eastern firms inside and outside Iran.”¹⁸¹

536. On August 30, 2012, MTN Group issued a statement to *Reuters*, in which “MTN denied any wrongdoing.”¹⁸² According to Reuters, “Paul Norman, MTN Group’s chief human resources and corporate affairs officer,” issued a statement to *Reuters*:

MTN denies that it has ever conspired with suppliers to evade applicable U.S. sanctions on Iran or had a policy to do so. MTN works with reputable international suppliers. Our equipment is purchased from turnkey vendors and all our vendors are required to comply with U.S. and E.U. sanctions. We have checked vendor compliance procedures and continue to monitor them and we are confident they are robust.¹⁸³

537. MTN Group’s denial was a lie, and MTN Group intended to conceal MTN Group’s and MTN Dubai’s membership in the IRGC’s terrorist conspiracy, which MTN Group joined on behalf of itself and MTN Dubai in 2005, and from which MTN Group and MTN Dubai have yet to exit. MTN Group’s statement aided the IRGC’s terrorist finance and logistics scheme by engaging in strategic communications targeted at the United States, which maintained MTN Group’s status as a viable “cover” for the illicit fundraising and acquisition of embargoed American technologies by Hezbollah, the Qods Force, and Regular IRGC while MTN Group was under close scrutiny.

¹⁸¹ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

¹⁸² Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

¹⁸³ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

538. As the IRGC's chief outside telecommunications partner, MTN helped Hezbollah, the Qods Force, and Regular IRGC grow their cellular-phone capabilities, evade American sanctions, and acquire embargoed U.S.-made communications technology.

539. From 2005 through the present, MTN has illegally sourced embargoed dual-use U.S. technology at the request of Hezbollah, the Qods Force, and Regular IRGC in coordination with MTN's Qods Force handlers in the U.A.E., where MTN and Hezbollah, the Qods Force, and Regular IRGC coordinate their technical collaboration. Plaintiffs' belief is based upon, among other things, information and inferences based upon statements made by one or more witnesses, MTN's own internal documents, financial records, and investigations by major global media outlets.

540. For example, on June 4, 2012, *Reuters* reported on MTN leading efforts to illegally acquire hundreds of dual-use, military-grade embargoed communications, telecom, and computer technologies for Hezbollah, the Qods Force, and Regular IRGC:

A fast-growing Iranian mobile-phone network managed to ***obtain sophisticated U.S. computer equipment despite sanctions that prohibit sales of American technology to Iran***, interviews and documents show. MTN Irancell, a joint venture between MTN Group Ltd of South Africa and an Iranian government-controlled consortium, sourced equipment from Sun Microsystems Inc, Hewlett Packard Co and Cisco Systems Inc, the documents and interviews show. MTN owns 49% of the joint venture but provided the initial funding. ...

Chris Kilowan, who was MTN's top executive in Iran from 2004 to 2007, said in an interview ... [that] ***MTN's parent company, MTN Group, was directly involved in procuring U.S. parts for MTN Irancell***, which launched in 2006 and is now Iran's second-largest mobile-phone operator. ***"All the procedures and processes around procurement were established by MTN,"*** he said. He said the company ***agreed to allow its Iranian partners and MTN Irancell*** to set up a local Iranian company with the ***"basic" purpose of evading sanctions on Iran.*** ...

Reuters provided MTN with the names of four current MTN Group executives believed to have knowledge of the procurement of U.S. parts by MTN Irancell. MTN declined to make any of them available for interviews. ...

Kilowan’s claims regarding how MTN Irancell obtained U.S. parts for its network ... were supported in documents and numerous interviews conducted by Reuters. For example, Reuters reviewed an 89-page MTN Irancell document from 2008 that shows the telecom carrier was specifically interested in acquiring embargoed products. ... In a section on managing product-support agreements for third-party equipment, *the MTN Irancell document states, “This should include embargo items.”* The document also includes *lists of network equipment, including Cisco routers, Sun servers and products from HP.* ...¹⁸⁴

541. *Reuters* “documented ... how Iranian telecoms - including the MTN joint venture – [] managed to obtain embargoed U.S. computer equipment through a network of Chinese, Middle Eastern and Iranian firms.”¹⁸⁵ As *Reuters* put it, “[t]he Turkcell-MTN case offers further evidence that there are always companies willing to do business with a country even when it becomes an international pariah.”¹⁸⁶

542. MTN’s technical assistance to Hezbollah, the Qods Force, and Regular IRGC had a devastating impact on the U.S. government’s ability to protect Americans in Afghanistan from al-Qaeda and Taliban terrorist attacks. By helping to revolutionize the IRGC’s communications capabilities, MTN helped Hezbollah, the Qods Force, and Regular IRGCs better conceal their communications with their proxies inside Afghanistan to make it nearly impossible for American counter-terror forces in Afghanistan to monitor the IRGC-backed terrorists attacking Americans in there. By making it easier for Hezbollah, the Qods Force, and Regular to securely communicate with one another, and the IRGC’s proxies in Afghanistan, MTN made it easier for al-Qaeda and the Taliban to attack Americans – and they did. MTN accomplished this

¹⁸⁴ Steve Stecklow, *Exclusive: Iranian Cell-Phone Carrier Obtained Banned U.S. Tech*, Reuters (June 4, 2012) (emphasis added; formatting adjusted).

¹⁸⁵ Steve Stecklow and David Dolan, *Special Report: How An African Telecom Allegedly Bribe Its Way Into Iran*, Reuters (June 15, 2012).

¹⁸⁶ *Id.*

“communications concealment” assistance to Hezbollah, the Qods Force, and Regular IRGC which flowed through to al-Qaeda and the Taliban in at least three ways.

543. *First*, MTN acquired advanced American-made encryption technologies for Hezbollah, the Qods Force, and Regular IRGC, which flowed through to al-Qaeda and the Taliban, including its Haqqani Network. The terrorists used the MTN-acquired, U.S.-manufactured and embargoed technologies to encrypt their communications.

544. *Second*, MTN sourced more than one thousand (1,000) advanced, encrypted American smart phones each year from 2006 through 2017 that were intended to be used, and were in fact used, by Hezbollah, the Qods Force, and Regular IRGC, for terrorism targeting Americans. The American smart phones sourced by MTN for Hezbollah, the Qods Force, and Regular IRGC, were used to increase the effectiveness of IRGC-funded (including and Qods Force-funded) IEDs in Afghanistan by making it easier for terrorists to detonate them and harder for American counter-IED technologies to prevent their detonation by “jamming” them.

545. *Third*, MTN lied to the U.S. government about its ongoing cooperation with and work on behalf of Hezbollah, the Qods Force, and Regular IRGC. This furthered al-Qaeda’s and the Taliban’s terrorist campaign in Afghanistan by preventing the U.S. government from knowing and understanding what technology the terrorists had, and when it was obtained.

546. Even as of the date of this Complaint, MTN continues to dissemble about its relationship with Hezbollah, the Qods Force, and Regular IRGC. Even after the United States designated the IRGC as a Foreign Terrorist Organization on April 19, 2019, MTN stubbornly refused to acknowledge any need to change its business practices in Iran for more than a year, instead rolling out a host of new offerings designed to *increase revenue* flowing to MTN Irancell and, by extension, the two newly-designated-FTO-fronts that controlled MTN Irancell.

547. Finally, on August 6, 2020 – *475 days after the IRGC’s FTO designation* – MTN announced that it was exiting the Middle East. Even then, however, MTN refused to condemn Hezbollah, the Qods Force, and Regular IRGC refused to promise a rapid withdrawal from its terrorist joint venture, MTN Irancell, and merely offered a blithe promise that MTN would eventually exit MTN Irancell in four or five years (i.e., sometime in 2024 or 2025).

548. On information and belief, MTN declined to immediately exit its joint venture with two FTO fronts after the IRGC’s FTO designation because MTN determined that MTN would lose, at least, hundreds of millions of dollars if MTN rapidly withdrew from its MTN Irancell joint venture with the Bonyad Mostazafan and IEI.

549. As alleged, MTN knew, or recklessly disregarded, that it was dealing with Qods Force fronts, but given the IRGC’s designation as an FTO in 2019, MTN’s ongoing relationship with two widely recognized IRGC fronts proves MTN deliberately chose to join the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist enterprise against the United States, which MTN self-evidently views as an acceptable cost of doing business.

550. MTN’s ongoing refusal in 2021 to immediately and unconditionally (as in weeks, not months or years) exit its joint venture with fronts for Hezbollah, the Qods Force, and Regular IRGC even after the IRGC had been designated as an FTO in 2019, and nearly every other multinational corporation had withdrawn from such joint ventures with Iranian fronts nearly a decade earlier, further confirms that MTN meant to support Iran-backed terror all along. The following history of the UANI’s public pressure campaign demonstrates this.

551. On January 25, 2012, Ambassador Wallace, the president of UANI, wrote to Sifizo Debengwa, MTN Group’s then-President and CEO:

[UANI] is writing to express its concern about the ongoing business of [MTN] in Iran. Recently, UANI launched its “Tech and Telecom Campaign” to highlight

the Iranian regime's misuse of technology ... In response ..., a number of corporations, including Huawei and Nokia Siemens Networks ("NSN"), have curbed their business activities in Iran. We now ask MTN to do the same.

The reasons for this call by UANI are manifold. ... Iran [] remains the *world's leading state sponsor of terrorism and has sponsored notorious terrorist groups like ... Hezbollah.... Iran's ... terrorist activities should be reason enough for a corporation to pull out of Iran....*

MTN is a 49% shareholder of MTN Irancell, the second largest mobile phone network operator in Iran. The majority 51% is in turn owned by the Iranian regime, which has exploited the network and telecommunication technology of MTN Irancell ...

In addition, in 2009 MTN Irancell bought a mobile-positioning center from Ericsson. Iranian security forces have reportedly utilized such mobile positioning centers to pinpoint the location of mobile telecommunications users. (Bloomberg, "Iranian Police Seizing Dissidents Get Aid of Western Companies," 10/30/2011) More recently, MTN Irancell reportedly purchased a system from Creativity Software that enables Iranian security forces to monitor the location of cellular phone users. The system also stores data and can generate reports about a person's movements. (Bloomberg, "Iranian Police Seizing Dissidents Get Aid of Western Companies," 10/30/2011) As co-owner of MTN Irancell, MTN certainly had knowledge of such purchases and by collaborating directly with the Iranian regime, MTN is complicit in facilitating the abuses that occurred ... as a result.

In short, it appears that MTN is taking advantage of the fact that responsible corporations are leaving Iran, and eagerly filling the void. MTN must end its irresponsible business practices in Iran and, in particular, its direct collaboration with the Iranian regime. ... [Emphasis added.]

552. On February 29, 2012, Ambassador Wallace followed up on his January 2012

letter to MTN Group's President and CEO:

[MTN] fails to respond to evidence of Iran's routine use of telecommunications equipment to illegally track, monitor, and in some cases arrest, detain, and torture Iranian citizens opposed to the current extremist regime. More specifically, [MTN] also fails to refute the fact that the Iranian regime, the majority 51% holder of Irancell and partner of MTN, "has exploited the network and communications of peaceful dissidents in Iran." Finally, [MTN] fails to respond to UANI's inquiries regarding multiple reports of collaboration by MTN Irancell and the Iranian regime ... MTN is a 49% shareholder of MTN Irancell, and the majority 51% is in turn owned by the Iranian regime. ***This means that MTN's "partner" in MTN Irancell is the Iranian regime. ...***

In addition, given MTN's relationship with the regime, MTN's assertion that it is a "liberating force," "enriching the lives" of Iranians is completely untenable. MTN cannot reasonably assert that the substantial profits it earns from its growing role in the Iranian telecommunications market are merely a byproduct of a larger altruistic goal to empower the citizens of Iran and the developing world....

Recent reports in the news media regarding MTN's Iran business further belie MTN's assertion that its business in Iran is altruistic or ethical in nature. For example ***MTN Irancell's other Iranian partial owner is the Mostazafan Foundation of Islamic Revolution, a "Bonyad" organization directly supervised by Iran's Supreme Leader. Both IEI and Mostazafan are closely linked to the regime's radical [IRGC].*** ... [Emphases added.]

553. MTN's President and CEO responded to UANI in an on-the-record interview with the *Wall Street Journal*, during which MTN's CEO stated: "What the [Iranian] government decides to do with that equipment ***is not in our hands***. We cannot say who they listen to and when."¹⁸⁷ In the same 2012 article regarding that interview, the *Journal* reported that:

MTN Group Ltd. will leave Iran ***only if*** South Africa applies sanctions on the country, Chief Executive Sifiso Dabengwa said Wednesday. The South African telecom company is facing international pressure to pull out or scale down operations in Iran ... "We are guided by South African government policies internationally," Mr. Dabengwa said, noting that the country hasn't imposed sanctions on Iran. MTN has a 49% stake in Iran's second-largest mobile-phone operator and derives 21% of its subscriber base from Iran, according to recent figures from MTN. ...¹⁸⁸

554. On March 7, 2012, Ambassador Wallace, the president of UANI, publicly responded:

The facts are clear: MTN is partners with sanctioned Iranian entities with direct links to the IRGC. ... If MTN does not respect its own stated corporate values, it should ... respect the will of the international community, which is working to isolate the Iranian regime in response to its ... ***support of global terrorism*** ...

¹⁸⁷ Devon Maylie, *South African Wireless Firm MTN To Remain In Iran*, Wall St. J. (Mar. 8, 2012) (emphasis added).

¹⁸⁸ *Id.* (emphasis added).

Investors and affiliated institutions should immediately divest themselves from MTN until MTN ceases its complicity with the Iranian regime.¹⁸⁹

555. On March 12, 2012, MTN Group issued a press release that stated, in part: “On human rights, the [MTN] group takes direction from and adheres to the policies of both the South African government and the United Nations. South Africa has human rights enshrined as fundamental principles within its Constitution.” MTN then shamefully invoked South Africa’s history of apartheid to suggest that it was a responsible corporate citizen, stating: “Given South Africa’s own recent history and our struggle against apartheid, the centrality of civil rights is at the core of our culture as a company and as individuals.” MTN further defiantly – and absurdly – claimed that there was no “evidence that the Iranian government has used the data [MTN] collected [and shared with the IRGC via Irancell] to identify and locate citizens or dissidents.”

556. After issuing its press release, MTN subsequently scrubbed any presence of it from MTN’s websites. On information and belief, MTN did so because it knew that its statement was a damaging admission that MTN believed that although it was violating U.S. law, it could not be held accountable under U.S. law regardless of what it did with Iranian terrorist fronts like Hezbollah, the Qods Force, and Regular IRGC.

557. On March 14, 2012, Ambassador Wallace, the president of UANI, replied to MTN’s March 12, 2012 press release, in part by stating:

If MTN was serious about respecting human rights, it would withdraw from Iran ... Respecting human rights would also mean not trying to whitewash what MTN is really doing in Iran. MTN is not a liberating force for the Iranian people, as it claims. On the contrary, MTN is partnered with sanctioned Iranian entities with direct links to the IRGC, and has provided the regime with location data on

¹⁸⁹ UANI, *UANI Responds to MTN CEO’s Irresponsible Position on Iran and Renews Call for MTN to End its Business in Iran* (Mar. 7, 2012) (emphasis added); see Business Wire, *UANI Responds to MTN CEO’s Irresponsible Position on Iran and Renews Call for MTN to End its Business in Iran* (Mar. 7, 2012) (broad international publication of this UANI press release).

Iranian citizens ... MTN must end its irresponsible business in Iran, and stop contributing to the regime's continual human rights violations.¹⁹⁰

558. On March 28, 2012, Turkcell filed suit against MTN Group in United States District Court for the District of Columbia. *See* Complaint [Dkt. 1], *Turkcell İletişim Hizmetleri A.Ş. and East Asian Consortium B.V v. MTN Group, Ltd. and MTN International (Mauritius) Ltd.*, No. 1:12-cv-00479-RBW, (D.D.C. Compl. Filed Mar. 28, 2012) (“*Turkcell v. MTN*”).¹⁹¹ In its complaint (at 1), Turkcell alleged that MTN “violat[ed] ... the law of nations through bribery of sitting Iranian ... officials and trading influence to steal the first private Iranian Global System for Mobile Communications (“GSM”) license (the “License”) from Turkcell,” which included MTN’s “promis[e] [to] Iran [MTN would source] defense equipment otherwise prohibited by national and international laws” and MTN’s “outright bribery of high-level government officials in both Iran and South Africa,” which “acts ... deliberately resulted in Turkcell losing its rightfully-won valuable telecommunications opportunity and in MTN’s taking over the License.”

559. In its complaint (at ¶ 9), Turkcell alleged that, “[b]etween the end of 2004 and receiving the License in November 2005, MTN through ‘Project Snooker’ made at least five illegal bribes and trades in influence to government officials with the intention and belief that the bribes would cause the Iranian government to grant the License to MTN rather than Turkcell.”

- Paragraph 9(B) – labeled “Illicit Arms for the GSM License” – alleged that “MTN struck a deal to deliver ‘The Fish’ the Iranian Ministry of Defense in August 2004. ‘The Fish’ was a code name for a combination of military cooperation and big ticket defense equipment, including ... frequency hopping encrypted military radios, sniper rifles, ... radar technology, ... and other defense articles—particular items including U.S. systems or components. This equipment

¹⁹⁰ UANI, *UANI Responds to MTN's Claims that it Adheres to UN Human Rights Policies* (Mar. 14, 2012); *see* Business Wire, *UANI Responds to MTN's Claims that it Adheres to UN Human Rights Policies* (Mar. 14, 2012) (broad international publication of this UANI press release).

¹⁹¹ Turkcell subsequently voluntarily dismissed the case to pursue the matter in South Africa. *See* Notice of Voluntary Dismissal (Dkt. 47) and Minute Order (Dkt. 48) in *Turkcell v. MTN*, No. 1:12-cv-00479-RBW (D.D.C. May 1, 2013).

was unavailable to Iran through legitimate means because of U.S. and international restrictions at the time. MTN officials ... promise[d] delivery of the illicit [i.e., illicit] arms and technology in exchange for the License.”

- Paragraph 9(C) – labeled “Bribe of Iranian Deputy Foreign Minister” – alleged that “MTN promised in May 2005, and later paid through a sham consultancy, the Iranian Deputy Foreign Minister, Javid Ghorbanoghli, \$400,000 in U.S. dollars for his efforts to politically undermine and destroy Turkcell’s position as the license-holder and to deliver the License to MTN.”
- Paragraph 9(D) – labeled “Bribe of South African Ambassador to Iran” – alleged that, “[i]n June 2005, MTN promised, and later paid, the South African Ambassador to Iran, Yusuf Saloojee, the equivalent of U.S. \$200,000 to help MTN deliver on the nuclear vote and the weapons trafficking and to support MTN within the Iranian government. Ambassador Saloojee was integral to MTN’s ultimate success in securing the License.”
- Paragraph 9(E) – labeled “Bribes of Iranian Defense Organizations” – alleged that, “MTN promised the Iranian Ministry of Defense through its state-owned defense company Sairan (also known as Iran Electronics Industries or ‘IEI’) and the ‘Bonyad’ (one of the five Iranian quasi-independent ‘Charitable Foundations,’ an organization integral to the Iranian defense establishment), that MTN would pay all of Sairan [i.e., the IEI’s] and the Bonyad’s 51% share of the €300 million license fee, plus its entire capitalization cost and a share transfer tax, in exchange for their assistance within the Ministry of Defense and with the Supreme Leader. MTN later paid these amounts. These promises and payments, made through sham loans MTN knew at the time would not be repaid, were essential to MTN’s takeover of Turkcell’s License.”

560. Turkcell’s complaint against MTN also specifically alleged that MTN had engaged with an IRGC-controlled company. For example, Turkcell alleged that to

establish[] itself within Iran[,] ... [MTN] reached out to ... Mr. Mohammed Mokhber, the Deputy President of a major “charitable foundation” controlled by the Supreme Leader of Iran, known as the Bonyad Mostazafan (“the Bonyad”), which is ... ***controlled by the Iran Revolutionary Guard Corps***, the Iranian military complex formed by Iran’s Supreme Leader Ayatollah Ali Khamenei, which is believed to control approximately one third of the Iranian economy. ... The Bonyad ***reports directly to the Supreme Leader*** and MTN was confident that its relationship with Mr. Mokhber and the Bonyad he controlled provided direct access to the Supreme Leader. ***The Bonyad is well known for engaging in “Iran’s shadow foreign policy.”***

Id. ¶ 65 (emphasis added; citations omitted).¹⁹²

561. Turkcell’s complaint against MTN alleged that MTN’s senior executives, including its CEO, met with Iranian agents in South Africa (whom, Turkcell alleged, MTN invited to South Africa on a “trip” that “MTN funded”), during which time MTN’s executives “[t]ogether [] promised [the Iranian agents] that South Africa would deliver ‘heaven, earth, and the fish,’ meaning whatever military equipment [Iran] desired.” *Id.* ¶ 93. Turkcell continued: “The entire trip was organized and coordinated by MTN so that they could corruptly induce the Iranian government to eliminate Turkcell ... and replace it as the owner of the GSM opportunity.” *Id.*

562. On April 5, 2012, the *Mail & Guardian Centre* for Investigative Journalism in South Africa published a detailed expose on MTN’s partnership with Iranian terrorists, titled “Iran ‘Puts the Screws’ on MTN,” which reported that MTN “fac[ed] a storm over claims that it helped the Iranian government in 2009 and 2010,” and reported that:

Sources close to MTN’s Iranian business have [] described ***an Orwellian environment in the company’s Tehran headquarters***, where it allegedly ***gave military intelligence officials “open” access*** [S]ources claimed:

- Because MTN Irancell and its data centre were part-owned by the Iranian military, subscriber data was shared “on a collegial basis” with the intelligence sector;

¹⁹² Similarly, Turkcell also alleged (at ¶ 86), that “[t]hroughout 2004 and 2005, MTN regularly met with ... the Bonyad [Mostazafan] and Sairan [i.e., IEI],” during which time MTN’s “goal was to entice those entities to support MTN and abandon Turkcell, on the promise that MTN had more to offer than Turkcell.” *Turkcell v. MTN* Complaint at ¶ 86. Turkcell continued: “The Bonyad and [IEI] responded exactly as MTN planned: They not only used political leverage to increase delay and shift Turkcell’s regulatory requirements, but also they directly began disengaging from their relationship with Turkcell. After mid-2005, the Bonyad and [IEI]’s involvement with Turkcell was merely a charade along the path to forming its venture with MTN.” *Id.* ¶ 86.

- A shadowy ***“second floor” in MTN’s building was populated by military intelligence officials***, the volunteer militia known as the Basij (“morality police”) and clerics;
- During the 2009 and 2010 Green movement protests, men from the second floor, accompanied by Irancell chief executive Alireza Dezfouli, allegedly approached data warehouse staff regularly to demand detailed records for individuals;
- In one case, they demanded the number of a known Green Party activist, who could not be reached after his information had been given to military intelligence; and
- Third parties listened in to staff calls over Irancell SIMs and would intervene and demand that the staff speak in English and not in other South African languages. ...

[Turkcell’s lawsuit] accuses MTN of bribing South African and Iranian officials, facilitating weapon trade agreements between the two countries and influencing South African foreign policy ... in a bid to stop Turkcell from being awarded a second cellular network licence in Iran. ... MTN is a 49% shareholder in Iran-cell. Fifty-one percent is held by an Iranian state-linked consortium, which is dominated by a subsidiary owned by the defence ministry known as Sairan, or Iran Electronics Industries. Sairan is subject to US and European Union sanctions that target proliferators of “weapons of mass destruction”. It also holds a share in consortium Arya Hamrah, which owns and runs MTN Irancell’s data centre that houses the company’s servers and hardware. ...

Military intelligence

The sources familiar with MTN’s Iranian operations said that, because of these ownership structures, Irancell readily gave information about subscribers to intelligence officials. ... One of the sources said: ***“MTN’s data centre in Iran is effectively run by the military and military intelligence. None of the intelligence organisations needs to go through normal procedures to access subscriber data and track individuals.”***

Describing the climate at MTN’s headquarters, a senior official said it was ***dominated by the presence of Iran’s military intelligence officials and the “morality police”.***

“There was a tea lady who just stood at the printer all day. Her job was to watch us.” The woman, understood to be a member of the “morality police”, would scold female staff whose clothing was considered too revealing and signaled her displeasure over “inappropriate” behaviour.

Communicating by email, the source said: “The people on the second floor are from military intelligence and the Basij and some clerics. They oversee the intelligence and moral activities of the employees of Irancell. All emails, telephone conversations and SMSes of employees are monitored on an ongoing basis. This is then exposed to MTN against the threat that they will kick out MTN when they need concessions from it.”

The staffer described how men from the second floor would accompany Dezfouli to collect data on individuals and political dissidents: “On several occasions someone from the second floor and [Dezfouli] would come to the managed services group and say ‘give us all the details for this number’, and they would have to.” The staffer said subscription and location data and call and SMS histories were handed over. ...¹⁹³

On information and belief, the *Mail & Guardian*’s investigative report accurately described operations at MTN Irancell.

563. Shortly before the *Mail & Guardian*’s investigative piece was published, MTN issued a written statement to the *Mail & Guardian* from MTN Human Resources Head Paul Norman that was replete with falsehoods designed to conceal MTN’s ongoing joint venture with Hezbollah, the Qods Force, and Regular IRGC including MTN’s awareness that such a business partnership could conceivably result in violence. In that statement, MTN’s head of HR stated:

MTN’s role in Iran is mostly as a technical partner. It is a non-controlling shareholder. Fewer than 30 MTN expats (not all South African) are employed in Irancell, out of around 2000. ... MTN works hard, with international legal advisors, to ensure that it is sanctions compliant. ... Civic and human rights are vital to the company ... We expect all our business partners to abide by our code of ethics. Mobile telecoms has been a force for political and economic liberation ... But we accept the ethical complexities around telecoms in this new environment, and the potential for their manipulation for unethical means.¹⁹⁴

564. MTN remained defiant even though nearly every other major multinational corporation exited their own joint ventures with fronts for Hezbollah, the Qods Force, and

¹⁹³ Craig McKune and Sharda Naidoo, *Iran ‘Puts the Screws’ on MTN*, *Mail & Guardian* (Apr. 5, 2012) (emphases added).

¹⁹⁴ *Id.*

Regular IRGC after the Bush and Obama administration ramped up sanctions enforcement in the 2000s. As Ambassador Wallace explained in May 2012,

despite the action of other responsible telecommunication companies, South African telecom company MTN continues to openly partner with sanctioned Iran entities affiliated with the brutal Iranian regime. ***Companies like MTN deserve the condemnation of the American public and concerned citizens worldwide as well as the attention of this Congress, which should investigate MTN's collaboration with the Iranian regime.*** Nevertheless, UANI will continue to educate citizens and apply pressure against recalcitrant companies that pursue short-term profits at the expense of global security.¹⁹⁵

565. Even after a decade of Iran-backed terrorism against the United States, MTN's President and CEO told interviewers in 2013 that the company had no regrets about doing business with the Iranian and Syrian regimes that sponsored anti-American terror. As the *Financial Times* reported at the time, "[y]et [MTN's CEO] Mr Dabengwa says MTN has few regrets about entering Iran or Syria and includes them among countries that will be important to MTN's growth. 'The starting point for entering frontier markets is the business case. ***The other risks, we can manage,***' he says."¹⁹⁶ This view reflected MTN's corporate DNA that emphasizes taking risks that the rest of the industry thinks are too great: "Venturing into areas where others might fear to tread is a characteristic that has been at the heart of MTN's rapid expansion since it was established in 1994, the year South Africa held its first democratic election."¹⁹⁷

566. As the *Financial Times* reported in 2013, even the prospect of "deadly conflict" did "little to diminish MTN's appetite for risk."¹⁹⁸ Indeed, MTN's CEO admitted, in effect, that MTN believed that American lives in Afghanistan and Iraq did not count in MTN's calculations.

¹⁹⁵ Wallace May 17, 2012 Testimony (emphasis added).

¹⁹⁶ Saigol and England, *Telecoms: Dealings in the Danger Zone*.

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

Specifically, commenting on how MTN operates in conflict zones, MTN's President and CEO stated: "I would say, is our presence there enhancing anybody's position in this conflict? That, for me, would be the test. If you could turn around and say our presence there is enhancing the government's position or it's enhancing the other side's position, then I guess it's an issue. Walking out today is not an option."¹⁹⁹

567. On or about November 2012, the Treasury Department announced additional sanctions targeting the IRGC's use of the telecommunications industry to help inflict violence upon innocent civilians. As was reported in real time by the South African media, MTN understood that these new Treasury sanctions punished MTN's counterparty for its support of terrorism. For example, according to the South African financial publication *Fin24*, these "[s]anctions announced ... by the US treasury against Iranian individuals and companies have led to panic at mobile operator MTN," because MTN "believed" that the Treasury announcement "target[ed] 17 individuals believed to be related to human rights abuses by the Iranian government, as well as to supporting terrorism and the Islamic Revolutionary Guard."²⁰⁰ As *Fin24* reported at the time, "the mobile operator [was] concerned sanctions will cause a hardening of attitudes in the US against the company," which was problematic for it as "MTN [was] being sued in the US for allegedly bribing Iranian officials to obtain an operating licence, while it [was] negotiating with the US treasury to allow the operator to expatriate its cash profits from Iran before the Iranian rial completely bottom[ed] out."²⁰¹

¹⁹⁹ *Id.*

²⁰⁰ *Fin24, Panic at MTN Over US Treasury Sanctions* (Nov. 11, 2012).

²⁰¹ *Id.*

568. Incredibly, even after MTN understood the Treasury Department to be sanctioning its business partners in Iran for sponsoring terror, MTN sources still complained to the media about the audacity of the United States expecting MTN to follow U.S. law. As one anonymous “MTN source[]” complained to *Fin24* that “[t]his is a [South African] company that ***should not be subjected to US foreign policy decisions.***”²⁰²

569. By the end of 2012, MTN was nearly alone (joined by ZTE, among others) as one of the few large multinational corporations that remained willing to work – openly or surreptitiously – as an IRGC, including Hezbollah and the Qods Force, joint venture partner. As Nathan Carleton, communications director for UANI, summed it up at the time “MTN stands out as one of the single most irresponsible businesses in the world and should be ashamed of the depths it has gone to in pursuit of profit.”²⁰³

570. MTN is virtually alone in the corporate world as a multinational corporation that rarely explicitly and unambiguously condemns terrorist violence against Americans, for the obvious reason that openly condemning anti-American terror would anger MTN’s joint venture partners in Iran. Instead of expressing any sympathy for Americans killed and maimed in Afghanistan and Iraq – which, on information and belief, MTN never publicly did prior to being sued by victims of Taliban terrorism in 2019 – MTN instead showered its business partner, Ayatollah Khamenei, with adulation. For example, MTN Irancell was the lead sponsor of an Ayatollah-backed contest, which MTN Irancell as offering a chance “to visit the Supreme Leader of the Islamic Revolution Ayatollah [] Khamenei during [the competitors’] stay in Tehran.”²⁰⁴

²⁰² *Id.* (emphasis added).

²⁰³ *Id.*

²⁰⁴ Tehran Times, *Reciters From 75 Countries to Participate in Tehran Quran Competition* (May 14, 2015), 2015 WLNR 14128237.

4. MTN Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq

571. MTN has become one of the world's most valuable telephone companies by “wading into nations dealing with war, sanctions and strife.”²⁰⁵ Success in unstable markets, including Afghanistan, has yielded profits. MTN is now, due to this business model, “bigger by some measures than its U.S. counterparts.”²⁰⁶

572. MTN followed that model in Afghanistan. In mid-2006, MTN Group bought Areeba, a Lebanese telephone company that had recently won a license to provide cellular-telephone service in Afghanistan. MTN entered the Afghan market shortly thereafter and began as the country's third-largest provider (consistent with its status as the third entrant), well behind the two incumbents. But MTN grew quickly, and by late 2010 it had obtained an estimated 32% market share – the largest of Afghanistan's then-five cellular-phone providers. As MTN grew, it rebranded Areeba as MTN Afghanistan, and it expanded its geographical footprint throughout the country. By 2012, MTN had a presence in virtually every province in Afghanistan, including many that were under Taliban control or influence.

573. While MTN was achieving rapid growth in Afghanistan, the cellular-telephone sector provided a critical source of financing for the Taliban. As reported by the *Wall Street Journal* in 2010, telephone industry executives themselves “say operators or their contractors routinely disburse protection money to Taliban commanders in dangerous districts. That's usually in addition to cash that's openly passed to local tribal elders to protect a cell-tower site –

²⁰⁵ Alexandra Wexler, *Telecom Giant Pushes Into Dangerous Areas*, Wall St. J. (Aug. 10, 2019).

²⁰⁶ *Id.*

cash that often also ends up in Taliban pockets.”²⁰⁷ “Coalition officers,” the article continued, “confirm that carriers make payments to the Taliban.”²⁰⁸ Those payments mirrored the protection money delivered by other Defendants. As terrorist-financing expert Thomas Ruttig documented, just as the Taliban raised “taxes” from international contractors doing business in Afghanistan, so too did it levy similar “taxes” on “the big telecom companies” like MTN.²⁰⁹

574. The logic behind MTN’s protection payments partially matched the logic motivating the other Defendants. The MTN Co-Conspirators intended to harm American interests in Afghanistan, and supporting the Taliban allowed them to do so. In addition, MTN had economic motivations similar to those of the other Defendants. Specifically, the Taliban asked MTN to “pay monthly protection fees in each province, or face having their transmission towers attacked.”²¹⁰ The going rate was “usually in the range of \$2,000 per tower, per month, but it depends on who controls the zone around each tower.”²¹¹ In some areas, MTN made payments to local Taliban commanders in exchange for protection. In others – such as Helmand and Kandahar – MTN operated in a Taliban-controlled environment in which protection “payments must go directly to Quetta.”²¹² For example, one company confirmed to *Deutsche*

²⁰⁷ Yaroslav Trofimov, *Cell Carriers Bow To Taliban Threat*, Wall St. J. (Mar. 22, 2010) (“*Cell Carriers Bow To Taliban Threat*”).

²⁰⁸ *Id.*

²⁰⁹ Thomas Ruttig, *The Other Side* at 20, Afghanistan Analysts Network (July 2009) (“*Ruttig, The Other Side*”).

²¹⁰ *Crime & Insurgency* at 32.

²¹¹ *Id.*

²¹² *Id.*; see *id.* (one company admitting it “routinely sen[t] a representative to Pakistan to pay off the Taliban leadership”).

Presse Agentur that it made \$2,000-per-tower monthly payments to the Taliban. The company's owner posited: "You have to do it. Everybody does."²¹³

575. The Taliban conveyed its protection-money demands to MTN and other large cellular-phone providers via Night Letters. Dr. Barnett Rubin, an Afghanistan policy expert, obtained a copy of one such letter in 2008 from an industry source and explained why "[s]etting up a cell phone tower anywhere in Afghanistan requires the consent of whoever 'controls' the territory, or at least has the power to blow [it] up."²¹⁴ As a result, cellular-phone companies in southern Afghanistan – where MTN had a heavy presence – typically believed they "ha[d] to pay the Taliban."²¹⁵ The *Financial Times* likewise reported in 2008 that Taliban commanders in Wardak Province had "sent letters to mobile phone companies demanding 'financial support' in return for operating" in Taliban-run areas.²¹⁶ Those tactics were successful. One industry source estimated in 2009 that "every single one of the shadow provincial governors set up by the Taliban leadership council receives \$50,000 to \$60,000 in protection money each month alone from the telecommunications sector, the largest legal growth market in Afghanistan."²¹⁷

576. The Taliban itself confirmed that practice. After the *Financial Times* obtained a copy of a Taliban Night Letter demanding protection payments from cellular-phone companies in Wardak Province, the reporter called the telephone number listed as the point of contact in the

²¹³ *How The Taliban Has Turned Extortion Into A Gold Mine.*

²¹⁴ Barnett Rubin, *Taliban & Telecoms – Secret Negotiations Just Got Easier, And At A Price You Can Afford!* (Mar. 31, 2008), icga.blogspot.com/2008/03/rubin-taliban-and-telecoms-secret.html.

²¹⁵ *Id.*

²¹⁶ Jon Boone, *Telecom Chief Says Rivals Pay Taliban Protection*, *Fin. Times* (June 9, 2008) ("Rivals Pay Taliban Protection").

²¹⁷ *How The Taliban Has Turned Extortion Into A Gold Mine.*

Taliban’s letter. A “local Taliban official” answered and confirmed that “two companies had responded to their demands” by agreeing to pay. On information and belief, MTN was one of them. The Taliban official explained: “When a company sets up they have to pay tax to the government of Afghanistan. . . . We are the government here and they must pay tax to us.”²¹⁸

577. MTN was a particularly aggressive practitioner of protection payments. Rather than invest in expensive security for its transmission masts, MTN purchased cheaper “security” by buying it from the Taliban. Indeed, MTN declined to use armed guards to protect its towers. Without paying for physical security, MTN both had the free cash flow and the incentive to buy peace with the Taliban. The CEO of one of MTN’s largest competitors, Roshan, alleged as much in 2008. According to an interview the CEO gave to the *Financial Times*, other “phone companies in Afghanistan [were] bowing to criminal and Taliban demands to pay protection money to avoid the destruction of their transmission masts.”²¹⁹ In the interview, Roshan’s CEO continued: “I believe the competition is paying money, but we don’t do that.”²²⁰ Of Roshan’s four largest competitors, three of them denied the accusation on the record. Only “MTN, the South African based multinational phone company, was not available for comment.”²²¹

578. MTN’s public statements reflect its practice of paying protection money. Because MTN paid the Taliban, it was, in its own words, “‘not a target.’”²²² According to an MTN

²¹⁸ *Rivals Pay Taliban Protection.*

²¹⁹ *Id.*

²²⁰ *Id.*

²²¹ *Id.*

²²² *Cell Carriers Bow To Taliban Threat.*

Afghanistan executive, “it’s enough for a driver to show at a Taliban checkpoint a company letter stating that equipment aboard the truck belongs to MTN and not to the U.S. forces.”²²³

579. MTN negotiated its protection payments in direct discussions between MTN Afghanistan’s security department and Taliban commanders. MTN’s security department consisted of roughly 600 total staff in Afghanistan, which included both local Afghan employees of MTN Afghanistan and a South African security component from MTN Group. The security department consisted of three different layers: provincial, regional, and a Tactical Operations Center in Kabul. Security personnel throughout those levels orchestrated pay offs to the Taliban. For example, one high-ranking MTN Afghanistan official conducted at least 38 telephone negotiations (which he recorded) with Taliban officials from 2007-2014, in which he engaged in so-called “security coordination” with the insurgency. The MTN employees who witnessed those conversations knew they were illegal, so they typically went to the roof of MTN Afghanistan’s Kabul headquarters building – where they could maintain absolute privacy – to conduct their Taliban negotiations in secret. In addition, on at least one occasion, MTN negotiated its payments at an in-person meeting held with Taliban officials near Quetta, Pakistan. MTN employees in Afghanistan understood that those negotiations involved MTN agreeing to make both cash payments and in-kind bribes (including equipment) to the Taliban.

580. The Afghanistan Threat Finance Cell (ATFC) gathered evidence from 2008-2012 confirming MTN Afghanistan’s practice of paying off the Taliban. The ATFC generated intelligence products, memorialized in DEA Form 6’s and Intelligence Information Reports, describing the common practice among Afghan telecommunications firms of paying the Taliban. According to the ATFC’s evidence, MTN Afghanistan was the worst offender of all the

²²³ *Id.*

companies. The ATFC confirmed MTN Afghanistan's frequent insurgent payments both in interviews with MTN employees and in wire intercepts collected by the Afghan government's Sensitive Investigative Unit. In witness interviews with ATFC investigators, MTN employees admitted that MTN Afghanistan paid insurgents not to threaten its cell towers. They justified those payments by appealing to MTN's commercial interests: MTN sources told the ATFC that it was cheaper to pay the Taliban than it would have been to rebuild the towers in the face of Taliban threats.

581. MTN's practice of making protection payments to the Taliban extended to the Haqqani Network. From at least 2010 through 2016, MTN operated towers in Haqqani-controlled territory in southeast and eastern Afghanistan, and it purchased security for those towers by paying the Haqqani Network. The Network's chief financial operative, Nasiruddin Haqqani, oversaw those payments, and they typically occurred on a semi-annual basis.

582. The U.S. government strongly opposed MTN's practice of paying the Taliban. ISAF's leadership was aware of cell phone companies making protection payments to the Taliban and pressured the companies to stop. On information and belief, the U.S. government exerted that pressure in direct discussions between the U.S. government and MTN, and also through the Afghan Ministry of Communications. On one occasion, an ISAF commander raised the issue directly with President Karzai. In such conversations, ISAF's leadership specifically rejected the argument that protection payments represented an acceptable price of MTN maintaining its network in Afghanistan. ISAF and the Afghan government warned MTN Afghanistan that its business practices were supporting the insurgency and were threatening Coalition forces, and both entities instructed MTN to stop. MTN refused.

583. MTN supplied the Taliban with more substantial assistance than its competitors did. MTN's 2006 entry into Afghanistan set the stage for the Taliban's cellular-tower rackets by adding another participant to the Afghan cellular marketplace. Until that point, the Taliban's ability to extract money from the two incumbent providers had been limited. Once MTN emerged in 2006, it became the third cellular company in Afghanistan, which gave the Taliban additional leverage to execute on its protection racket. That is because, with MTN agreeing to pay the Taliban, the Taliban were free to follow through on its threats against other companies without the risk that doing so would cut off all cellular service in Afghanistan – service on which the Taliban itself relied. Indeed, because Taliban fighters commonly preferred to use MTN's network for their own communications, the Taliban did not want to destroy MTN's network.

584. A review of available cell-tower attack data supports the same conclusion. Plaintiffs have analyzed all of the available purported U.S. military Significant Activities reports, as published online, that describe attacks between 2004 and 2010 against or in the immediate vicinity of a cellular tower in Afghanistan. The data shows a clear disparity between MTN and its two main competitors, Roshan and Afghan Wireless Communication Company ("AWCC"). From 2004 to 2009, AWCC and Roshan suffered at least 6 and 7 attacks on their towers, respectively, whereas MTN – which did not even pay guards to protect its towers – faced only 1 (non-lethal) attack. The disparity is consistent with Roshan's accusation that MTN paid protection money to the Taliban.

585. That attack disparity existed despite MTN's and Roshan's deployment of transmission masts at similar times in similar locations. For example, Roshan's CEO cited to the *Financial Times* an instance on May 14, 2008, in which the Taliban attacked one of Roshan's towers in Wardak Province, yet two similar nearby towers (including one belonging to MTN)

were not attacked.²²⁴ The most likely explanation for the difference is that MTN had paid protection money, whereas Roshan had not. Indeed, in 2009, Roshan maintained company rules that prohibited it from paying protection money to terrorists. Because Roshan refused to pay, the Taliban destroyed 18 of Roshan's towers in and around the 2009 Afghan elections.

586. The senior MTN Afghanistan security official who oversaw many of MTN Afghanistan's protection payments to the Taliban reported directly to the head of MTN Group's head of business risk management, in Johannesburg, South Africa. MTN Group was specifically aware of, and approved, MTN Afghanistan's practice of paying the Taliban for security. In fact, MTN Group compensated MTN Afghanistan's security team with cash bonuses reflecting its success at resolving "security issues" involving the Taliban. Those bonuses typically had three levels: Level 1 (\$1,500, for local operatives); Level 2 (\$5,000, for regional operatives); and Level 3 (\$10,000, for national operatives). The head of MTN Afghanistan's security group received roughly \$66,000 in such bonuses during the relevant timeframe, which specifically compensated him for negotiating with the Taliban successfully. MTN Group even gave him an award for best "display[ing] the Group's values in MTN Afghanistan."

587. MTN's overall payments to the Taliban reached tens, if not hundreds, of millions of dollars. Applying the standard rate of \$2,000 per tower per month to MTN's collection of roughly 1,300 towers yields an estimated payment of \$2.6 million per month. At that rate, MTN's payments from 2007 through 2016 well surpassed \$100 million.

²²⁴ *Rivals Pay Taliban Protection.*

5. MTN's Acts In Furtherance Of The Conspiracy Had A Substantial Nexus To The United States

588. MTN's joint venture with the IRGC and its related assistance for al-Qaeda and the Taliban, relied on significant contacts with the United States. MTN Group was a key player in orchestrating both those U.S. contacts and MTN's material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban.

589. MTN employs a top-down management structure in which MTN Group centralizes operational control over the functions performed by its various subsidiaries. During the relevant timeframe, MTN Group divided responsibility for its subsidiaries into six business groups; MTN Irancell (and Afghanistan) fell under the purview of the Middle East and North Africa ("MENA") group. The MENA group's functional units resided in Dubai and reported directly to senior management in South Africa.

590. MTN Group made the decision to enter a joint venture with the IRGC, including its Hezbollah Division and Qods Force, in 2004, when it began plotting "Project Snooker" to eject Turkcell from the existing deal. As part of "Project Snooker" – negotiated and executed by MTN Group's senior management – MTN ejected Turkcell from Irancell. MTN Group later rebranded Irancell as MTN Irancell.

591. Because MTN's business model depends on unstable countries, including Iran, one of MTN Group's core management responsibilities is to manage operational and political risk in the countries MTN enters. Assessments of those risks occur both before the decision to enter a market – here, as MTN entered Afghanistan in the mid-2000s – and on an ongoing basis. In mitigating those risks – which here included designing a strategy for coordinating MTN's operational support for the IRGC, including its Hezbollah Division and Qods Force, in Dubai and Iran – MTN Group implemented a number of measures, including the "appointment of a

Group crisis manager”; the implementation of “physical and staff security measures”; and “[c]ontinual monitoring of the political environment in operating countries.”²²⁵ MTN Group, not its operating subsidiaries, decided to do business with the IRGC, and Qods Force, fronts, and developed MTN’s strategy related thereto.

592. Those policies required MTN Group’s close supervision of MTN’s payments to Qods Force fronts, operatives, and agents, and MTN Irancell’s joint venture with the IRGC. As explained above, MTN Group made the decision – and instructed its subsidiary – to enter into a joint venture with the IRGC, including its Hezbollah Division and Qods Force. MTN Group also approved its subsidiary’s practice of providing payments and operational support to the IRGC, including its Hezbollah Division and Qods Force, including sourcing hundreds of sensitive dual-use items for IRGC, including Qods Force fronts, operatives, and agents inside and outside Iran in Dubai to benefit the Iranian IRGC’s, including Qods Force’s, terrorist enterprise. Those decisions had a substantial connection to the United States for the reasons explained below.

593. As ZTE’s and Huawei’s co-conspirator in the IRGC Conspiracy, MTN Group also connected ZTE’s and Huawei’s support of the IRGC Conspiracy to the United States by obtaining technology and vital operational support in reliance on U.S. contacts. MTN Group and MTN Dubai orchestrated a complex scheme to surreptitiously supply technology and operational support for the MTN Irancell through various U.S. agents. In doing so, MTN Group and MTN Dubai tied MTN’s unlawful conduct to the United States in several ways.

594. Even while MTN Group was reaching into the United States to launch a multifaceted campaign to facilitate the flow of U.S. dollars to and from MTN Irancell, its CEO continued expressing his contempt for the United States. Instead of exiting MTN Group’s and

²²⁵ *Id.*

MTN Dubai's conspiracy with the IRGC, MTN Group's President and CEO defiantly pronounced that "U.S. sanctions should not have unintended consequences for non-U.S. companies."²²⁶ This public statement by MTN Group's President and CEO furthered the terrorist conspiracy because it concealed the existence of the conspiracy while simultaneously releasing specific IRGC disinformation.

i. From 2012 Through 2019, MTN Group Regularly Reached Into The United States In Order To Unlock The U.S. Financial System So That MTN Group Could Repatriate Hundreds Of Millions Of Dollars Out Of MTN Irancell

595. MTN Group and MTN Dubai regularly engaged in large six- and seven-figure U.S. dollar transactions that flowed through the New York financial system before leaving the United States to flow into accounts controlled by an IRGC "buffer" such as an agent, operative, cut-out, front, and Orbit companies.

596. MTN Group and MTN Dubai's use of the New York financial system was not incidental. On information and belief, beginning on or about 2012 and continuing through on or about 2019, MTN Group, MTN Irancell, and MTN Dubai routinely relied upon banks in New York to manage the cash flow of MTN Group, MTN Dubai, and MTN Irancell, which was its most important (and cash intensive) investment in the Middle East.

597. MTN Group established banking relationships with U.S. financial institutions and multinational financial institutions with U.S.-based subsidiaries or offices no later than 2013.

598. For example, MTN Group disclosed that it has a relationship with the Bank of New York, located at 101 Barclay Street, New York, NY 10286, as its depository bank. Similarly, in 2015, MTN Group disclosed its relationship with Citibank, whereby it guaranteed a

²²⁶ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

syndicated loan facility worth \$1 billion, the same facility from which MTN International (Mauritius) Limited, the MTN Group subsidiary used to make corrupt payments to Iranian officials, had drawn \$670 million.

599. Following the easing of sanctions, in January 2016, MTN focused on repatriating funds from Iran. Indeed, MTN Group saw the easing of sanctions as an opportunity to “normalize” its repatriation of monies from MTN Irancell.

600. On October 24, 2016, MTN Group admitted that “MTN has commenced the repatriation of funds from MTN Irancell to MTN Group.”²²⁷ On December 14, 2016, “Bloomberg report[ed] that MTN Group ... extract[ed] several hundred million dollars with the help of European banks, and it [was] looking to take a total of around USD1 billion by the end of March 2017,” which “include[d] a *USD430 million loan repayment from MTN* Irancell.”²²⁸

601. The MTN Irancell profits that MTN Group withdrew covered the period when nearly every Plaintiff was injured. When MTN Group coordinated a global strategy to facilitate the repatriation of its MTN Irancell profits, MTN Group reached into the United States to obtain an enormous benefit – the money it made – that was itself the motivation for the terrorist finance that killed and injured Plaintiffs.

602. On information and belief, MTN Group utilized its banking relationships with U.S. financial institutions and/or financial institutions with U.S. subsidiaries or offices, including but not limited to the Bank of New York and Citibank, to facilitate the repatriation of funds from MTN Irancell to MTN Group.

²²⁷ MTN Group Ltd., Mtn Group Limited - Quarterly Update For The Period Ended 30 September 2016, South African Company News Bites – Stock Report (Oct. 24, 2016).

²²⁸ CommsUpdate, MTN Extracts First Cash From Iran (Dec. 14, 2016), 2016 WLNR 38124973.

603. Each time MTN Group and MTN Dubai used New York's financial system, they did so in a context where they benefited from the New York financial system, and New York laws, and they knew that the New York financial system imparted extra value to every transaction based upon its stability and reputation.

ii. MTN Group Facilitated A \$400,000 Bribe That Flowed Through The New York Financial System To A Cut-Out For The IRGC And Into The Budget Of Hezbollah, The Qods Force, And Regular IRGC

604. MTN Group's U.S. contacts were essential to the initial bribe that allowed MTN Group to pilfer the Irancell license from Turkcell in the first instance and was the proximate and but-for cause of MTN Group's and MTN Dubai's subsequent ability thereafter to assist the IRGC, including its Hezbollah Division and Qods Force's, terrorist enterprise, and join the terrorist conspiracy.

605. MTN Group relied upon bank accounts in New York to complete the \$400,000 wire that MTN Group sent to a recipient in 2007 who acted on behalf of the IRGC, including its Hezbollah Division and Qods Force. That payment depended upon MTN Group's use of bank accounts in New York, which cleared the dollar transaction.

606. MTN Group caused the issuance of the \$400,000 wire to the cutout for the IRGC, including its Hezbollah Division and Qods Force, also aided the IRGC's, including the Qods Force's, efforts to covertly obtain U.S. dollars – the vital common currency of terrorist finance – to fund al-Qaeda and Taliban attacks against Americans in Afghanistan and Joint Cell attacks against Americans in Iraq.

607. It would be improper to suggest that the absence of a direct on-paper linkage between the IRGC's cutout and the IRGC plausibly suggests that the \$400,000 did not flow through to Hezbollah, the Qods Force, and Regular IRGC.

iii. MTN Group And MTN Dubai Conspired To Provide, And Did Provide, A Stable, Robust, And Devastating Pipeline Of Illicitly Acquired State-of-the-Art American Technologies To Hezbollah, The Qods Force, And Regular IRGC, Including Untraceable American Smartphones

608. MTN Group’s co-conspirators have already confessed to the crimes they committed in coordination with MTN Group’s joint offenses with MTN Group. For example, Mohammad Hajian testified “that he sold super-computers worth about \$14-million to ‘a South African cellphone company in Iran [a reference to MTN]’, rather than to the regime itself.”²²⁹ At the time, his “alleged co-conspirator [was] also on trial in the US on charges that he serviced embargoed US technology for a ‘front company’ of MTN Irancell.”²³⁰

609. Like MTN Group and MTN Dubai, Mr. Hajian’s legal “memorandum” “stated that the network was geared solely for a deal with MTN Irancell: ‘All the merchandise was for non-military use and was intended to facilitate a joint venture between a South African cellphone company and a non-governmental Iranian entity related to the provision of civilian cellular telephone service within Iran.’”

610. United States District Judge Virginia Hernandez-Covington rejected the suggestion that MTN Irancell was a civilian phone company that was not under the control of the IRGC, and “ruled that the “[e]nterprise level server”] equipment sold to MTN Irancell in 2009 ‘could be dangerous’ in Iran, whether controlled by the government or by MTN Irancell.”²³¹

²²⁹ Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

²³⁰ Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

²³¹ Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

611. Federal “[p]rosecutors” also rejected the suggestion that MTN Irancell was a civilian phone company that was not under the control of the IRGC, and told the district court “that the [‘e]nterprise level server’] equipment sold to MTN Irancell in 2009 could have military applications and be used to spy on citizens.”²³² Prosecutors explained: “Even if used by [MTN] Irancell now, Iran could redeploy the equipment at any time ... The equipment is capable of being used by Irancell, or others, to access private information about subscribers and possibly communications content.”²³³ Indeed, “[t]he equipment Hajian was found to have illegally sold included a Sun Microsystems M9000 ‘enterprise level server, the largest and most powerful Unix processor that Oracle Sun sells,” and a “Hitachi Data Systems array,” which prosecutors “described as having the capacity to support various applications and ‘store vast amounts of data useful for large companies and [defense] departments.’”²³⁴

612. After pointedly noting Judge Hernandez-Covington’s ruling that the provision of U.S.-sold enterprise level server equipment to MTN Irancell “could be dangerous,” the *Mail & Guardian* journalists who followed Mr. Hajian’s trial also rejected the suggestion that MTN Irancell was a civilian company rather than an IRGC front:

In any event, Hajian’s assertion that Irancell was a civilian, non-governmental partnership was *inaccurate*. Although MTN owns 49% of the company, the balance is held by a consortium owned by two state-linked partners. The first, the purportedly charitable Bonyad Mostazafan Foundation, is *understood to be controlled by the Iran Revolutionary Guard* and the second, the state-owned defence company Sairan, reports directly to Iran's minister of defence.²³⁵

²³² Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

²³³ Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

²³⁴ Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

²³⁵ Rowan Philp and Craig McKune, *US Trial Turns Heat On MTN*, Mail & Guardian (Feb. 15, 2013), <https://mg.co.za/article/2013-02-15-00-us-trial-turns-heat-on-mtn-1/>.

iv. MTN Obtained U.S. Technology For The Benefit Of Hezbollah, The Qods Force, And Regular IRGC

613. MTN's U.S. contacts were essential to the technological assistance it provided to the Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban. At all relevant times, MTN relied upon U.S. agents to illegally source dual-use technology from the United States that benefited the IRGC's terrorist enterprise, including attacks against Americans in Afghanistan that were committed by IRGC proxies al-Qaeda and the Taliban.

614. As a condition of its contract with the IRGC, including its Hezbollah Division and Qods Force, MTN promised to obtain embargoed U.S. technology to benefit the IRGC's, including the Qods Force's, terrorist enterprise.

615. Between 2009 and 2012, one or more purchasing agents working for the IRGC, including its Hezbollah Division and Qods Force, in the U.A.E. and elsewhere, spending money provided by MTN Group, and acting at the direction of MTN Group and its IRGC, including Qods Force, ally, collectively wired more than \$5,000,000 into the United States to associates in the U.S. who purchased embargoed technology for the IRGC's, including the Qods Force's benefit, which was then shipped from the U.S. to the U.A.E., where the IRGC, including its Hezbollah Division and Qods Force, assumed possession of the technology for use in its terrorist enterprise.

616. On information and belief, MTN and/or MTN's agents routed millions of dollars each year to its U.S. agents to pay for the embargoed dual-use U.S. technology it illegally obtained for the IRGC, including its Hezbollah Division and Qods Force, via transactions through the New York banking system, by causing money to be wired to MTN's U.S. agents to pay for MTN's U.S. agents to illegally obtain embargoed dual-use U.S. technology for the benefit of the Qods Force's terrorist enterprise.

v. MTN Obtained Essential U.S. Services That Aided Hezbollah's, the Qods Force's, and Regular IRGC's Terrorist Capabilities

617. MTN's U.S. contacts were also key to its ability to obtain technical support from U.S. persons operating inside America, without which the IRGC, including its Hezbollah Division and Qods Force, could not have derived the terrorist benefits they did from MTN Irancell including the cash flow, network reliability, and enterprise computing benefits.

618. Between 2009 and 2012, and on information and belief ever since the mid-2000s, MTN Irancell relied upon one or more U.S. persons to service MTN Irancell's enterprise-level computers and associated networks, relying on one or more U.S. persons to maintain MTN Irancell's network remotely from the U.S. and, on at least one occasion, having such U.S. person travel to meet with MTN's IRGC, including Qods Force, allies in the U.A.E. to provide training to the Qods Force. MTN, or agents acting at MTN's direction, sourced embargoed technology for the IRGC's, including the Qods Force's, benefits from, among others, Akbari, Patco, MSAS, and TGO.

619. MTN routed millions of dollars each year to its U.S. agents, and sourced the sensitive dual-use U.S. technology, via transactions through the New York banking system, by causing money to be wired to MTN's U.S. agents to pay for MTN's U.S. agents to provide services, or obtain sensitive dual-use U.S. technology, for the benefit of the IRGC's, including the Qods Force's, terrorist enterprise.

620. On information and belief, MTN and/or MTN's agents routed millions of dollars each year to its U.S. agents in order to pay for the technology support services it illegally obtained for the IRGC, including its Hezbollah Division and Qods Force, via transactions through the New York banking system, by causing money to be wired to MTN's U.S. agents to

pay for MTN's U.S. agents to illegally provide technological support to maintain MTN Irancell for the benefit of the IRGC's, including the Qods Force's, terrorist enterprise.

B. The ZTE Defendants

1. ZTE Joined The Terrorist Conspiracy

i. Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts Including But Not Limited To MTN Irancell, TCI, and Exit40, ZTE Agreed To Join A Company-Wide Conspiracy

621. MTN Group and ZTE Corp. followed the same IRGC playbook because they joined the same conspiracy. Reuters concluded that "MTN was not alone" because "other foreign companies, including" "China's ZTE Corp, [] helped Iran undermine increasingly tougher sanctions."²³⁶

622. ZTE and its subsidiaries, including ZTE USA and ZTE TX, entered into a conspiracy to provide U.S.-origin goods and services, in violation of U.S. sanctions, to TCI. The agreement was in the form of contracts that ZTE signed with TCI and, on information and belief, MTN Irancell and MCI. The conspiracy was adopted by ZTE's senior leadership and deployed throughout ZTE and its subsidiaries, including ZTE USA and ZTE TX.

623. On information and belief, ZTE and its subsidiaries, including ZTE USA and ZTE TX, entered into a conspiracy to provide U.S.-origin goods and services, in violation of U.S. sanctions, to Exit40. The agreement was in the form of contracts that ZTE signed with Exit40 and, on information and belief, MTN Irancell and MCI. The conspiracy was adopted by ZTE's senior leadership and deployed throughout ZTE and its subsidiaries, including ZTE USA and

²³⁶ Steve Stecklow, *How A Telecom Giant Got Round Sanctions On Iran*, Reuters (Aug. 30, 2012).

ZTE TX. Plaintiffs' belief is based upon MTN Group's retention of Exit40, which, on information and belief, was for the same purpose and in response to the same IRGC instruction.

624. On information and belief, ZTE's contracts with its IRGC-front Iranian counterparties all included pledges to assist with the "security" of Iran.

ii. ZTE, ZTE USA, And ZTE TX Each Made Overt Acts In Furtherance Of The Conspiracy

625. Each of the ZTE Defendants, ZTE, ZTE USA, and ZTE TX acted in furtherance of the conspiracy by, *inter alia*, (a) sourcing U.S.-origin technology, embargoed by the United States and useful to the terrorists, for export to Hezbollah, the Qods Force, and Regular IRGC (b) entering into contractual relationships with U.S. suppliers to acquire the "essential" technology needed by the terrorists, (c) developing and using third-party companies to both conceal and facilitate its business with IRGC-front companies, (d) comingling U.S.-origin technology with non-U.S.-origin technology in order to evade detection of the scheme and conspiracy, (e) lying to U.S. prosecutors and financial institutions regarding the nature of their activities in Iran and their true IRGC-front counterparties, (f) destroying evidence related to the scheme and conspiracy, and (g) moving one or more witnesses in the United States with knowledge of the scheme and conspiracy out of the jurisdictional reach of the United States.

2. ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In Hezbollah's, The Qods Force's, And Regular IRGC's Terrorist Enterprise Against Americans Worldwide

626. ZTE bid on and secured contracts worth hundreds of millions of dollars to install cellular and landline network infrastructure in Iran. ZTE knew that its counterparties were IRGC, including Hezbollah and the Qods Force, fronts, operatives, or agents. ZTE thereafter developed an elaborate system to fulfill those contracts using US-origin items, including dual-

use goods controlled by the U.S. government due to their terrorism applications. ZTE did this in collaboration with, and with the assistance of, ZTE USA and ZTE TX.

i. ZTE Corp., ZTE USA, And ZTE TX Knowingly Facilitated MTN Irancell And TCI's Acquisition Of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies

627. Before 2011, ZTE sourced U.S. technology for Hezbollah, the Qods Force, and Regular IRGC. A Department of Justice Press Release dated March 7, 2017 (the "March 2017 Press Release") stated that ZTE violated U.S. sanctions by sending U.S.-origin items to Iran. It also announced ZTE's guilty plea to those charges and agreement to pay the U.S. government \$892,360,065. ZTE repeatedly violated export controls and illegally shipped U.S. technology to Iran, according to the March 2017 Press Release. On information and belief, ZTE did so in collaboration with and with the assistance of ZTE USA and ZTE TX.

628. ZTE's, ZTE USA's, and ZTE TX's (after its formation) company-wide scheme to obtain U.S.-origin goods and to evade export controls to get telecommunications technology into the hands of Hezbollah, the Qods Force, and Regular IRGC lasted from as early as 2010 to as late as 2016. While ZTE TX was not formed until at least 2013, Plaintiffs allege that ZTE TX and its employees participated in the scheme thereafter.

629. The cell phone technology and equipment ZTE sourced from inside the United States was subject to the embargo imposed and enforced by the United States Government. ZTE thus violated export controls designed to keep sensitive American technology out of the hands of IRGC, including Hezbollah and the Qods Force.

630. Through this scheme between January 2010 and January 2016 ZTE exported over 20 million U.S.-origin items to Hezbollah, the Qods Force, and Regular IRGC with a value of approximately \$32,000,000. ZTE did so without obtaining proper export licenses.

631. To evade the U.S. embargo, ZTE devised a scheme whereby an “isolation company” would be the vehicle used to hide ZTE’s shipment of prohibited U.S. technology to Hezbollah, the Qods Force, and Regular IRGC.

632. In early 2011, when ZTE determined that the use of its original “isolation company” was insufficient to hide ZTE’s connection to the illegal export of U.S.-origin goods to Hezbollah, the Qods Force, and Regular IRGC ZTE re-evaluated its strategy. In September 2011, four senior ZTE managers signed an Executive Memo which proposed that ZTE identify and establish new “isolation companies” that would be responsible for supplying U.S. component parts necessary for projects in embargoed countries.

633. After an international publication in March 2012 publicly revealed ZTE’s sale of prohibited equipment to Iran, ZTE temporarily stopped sending U.S. equipment to Hezbollah, the Qods Force, and Regular IRGC.

634. But in July 2014, ZTE began shipping U.S.-origin equipment to Hezbollah, the Qods Force, and Regular IRGC once again without the necessary licenses. Thus, properly understood, ZTE’s temporary pause was not the rumblings of a corporate conscience causing it to separate from terrorists but, rather, an effort to pause their support while they assessed whether they could get away with it. Once ZTE believed it could, on or about 2014, they resumed their support for Hezbollah, the Qods Force, and Regular IRGC.

635. ZTE made these additional shipments by using a new “isolation company.” In the new version of the scheme, ZTE purchased and manufactured all relevant equipment – both U.S.-origin and ZTE-manufactured – and prepared them for pick-up at its warehouse by the new isolation company. The new isolation company then shipped all items to Hezbollah, the Qods Force, and Regular IRGC.

636. In the ZTE 2017 OFAC Settlement, ZTE, and its subsidiaries, including but not limited to ZTE USA and ZTE TX, admitted, in relevant part:

(i) From on or about January 2010 to on or about March 2016, ZTE, ZTE USA, and ZTE TX (starting on or after the date of its formation) together exported, sold, or supplied United States goods to Iran or the Government of Iran with knowledge that the goods were intended specifically for Iran or the Government of Iran and thereby evaded or avoided, attempted and/or conspired to violate, and/or caused violations of the prohibitions set forth in the ITSR.

(ii) ZTE, ZTE USA, and ZTE TX together engaged in at least 251 such transactions, and the total value of U.S.-origin goods in the 251 transactions constituting the apparent violations was \$39,622,972.

(iii) From approximately as early as November 2010 to approximately March 2016, ZTE's senior leadership developed and adopted a company-wide scheme (meaning ZTE USA and ZTE TX, starting on or after the date it was formed, were involved) to evade U.S. economic sanctions and export control laws.

(iv) ZTE's actions were developed and approved by the highest levels of its management and entailed the use of third-party companies to both conceal and facilitate its business with fronts for the IRGC, including its Hezbollah Division and the Qods Force.

(v) ZTE, ZTE USA, and ZTE TX together were "specifically aware of and considered the legal risks and consequences of violating U.S. economic sanctions and export control laws," and were "specifically aware" of the potential consequences "if the U.S. government learned of [ZTE]'s unauthorized reexportation of U.S.-origin goods to sanctioned countries, including Iran."

(vi) Despite recognizing that “violations of U.S. law would be ‘inevitable’ if ZTE exported and/or reexported U.S.-origin goods to Iran,” ZTE, ZTE USA, and ZTE TX (starting on or after the date of its formation) together reexported and supplied a substantial volume of U.S.-origin goods to Iran from at least January 2010 to approximately March 2016 and “pursued and developed an evasive practice of ‘risk avoidance’ by utilizing isolation companies and other concealment activities” to do so.

(vii) ZTE’s contracts with Iranian companies from 2010 and 2012 required ZTE to export and/or reexport goods, services, and technology to Iran with the purpose of enhancing Iran’s telecommunications infrastructure, which in turn required supplying and/or attempting to supply Iran with U.S.-origin goods subject to the U.S. Department of Commerce’s Commerce Control List for anti-terrorism, national security, regional stability, and encryption item purposes and enhancing the law enforcement surveillance capabilities and features of Iran’s telecommunications facilities and infrastructure.

(viii) ZTE temporarily ceased performance of one of its contracts with an Iranian company [TCI], when Reuters reported in March 2012 that ZTE was circumventing U.S. sanctions law to provide U.S.-origin goods to TCI, but ZTE resumed its unlawful activity thereafter and “would not ultimately cease its unlawful activity or cooperate with the U.S. government until on or about March 2016.”

(ix) ZTE informed the U.S. government agencies and the public in 2012 that it was winding down its reexports of U.S.-origin goods to Iran. However, approximately one year later in November 2013, ZTE resumed its unlawful business activities with Iran without updating or informing the U.S. government agencies of this change until on or about April 6, 2016.

(x) In connection with the decision to resume its business with fronts for the IRGC, including its Hezbollah Division and the Qods Force, in approximately November 2013, ZTE's highest-level leadership instituted directives authorizing various divisions of the company to surreptitiously resume business with those IRGC fronts, including by using a new third-party isolation company to conceal the resumption of prohibited activities from U.S. government investigators, the media, and others outside of ZTE.

(xi) ZTE USA and ZTE TX were directly implicated and directly participated in the scheme: (i) the ZTE 2017 OFAC Settlement Agreement, including its admissions of wrongdoing, was entered into by ZTE and its subsidiaries and affiliates, including ZTE USA and ZTE TX; (ii) the acts ZTE, ZTE USA and ZTE TX, agreed they had done included shipping embargoed items from the United States by comingling those items with foreign-made non-embargoed items; (iii) the conduct detailed therein as violations of the U.S. sanctions regime was done via activity within the United States, was described as a "company wide" scheme, and U.S.-origin goods were described as "essential," so on information and belief ZTE USA and ZTE TX participated directly in those activities; (iv) ZTE entered into contractual arrangements with U.S. suppliers, including Qualcomm and Broadcom, through and by ZTE USA, through which ZTE obtained the key technology for export to Iran; (v) an employee, on information and belief, of either a ZTE USA or ZTE TX, was instructed by ZTE in China to leave the United States based on conduct done within the United States; (vi) ZTE has disclosed publicly that the same individual, Cheng Lixin, was simultaneously an officer of ZTE and the CEO of ZTE USA; and (vii) on information and belief the ZTE USA and ZTE TX were subject to multiple law enforcement subpoenas and ZTE USA and ZTE TX facilities were searched by United States authorities related to wrongdoing done in the United States.

637. ZTE modernized telecommunications technology used by Iranian entities that were controlled by Hezbollah, the Qods Force, and Regular IRGC fronts, thereby pumping additional revenue into the coffers of Hezbollah, the Qods Force, and Regular IRGC and thereby the IRGC's proxies in Afghanistan, al-Qaeda and the Taliban.

638. ZTE, ZTE USA, and ZTE TX (after its formation) provided substantial banned technology to Iranian companies that were controlled by Hezbollah, the Qods Force, and Regular IRGC. Thereby, ZTE's illegally sourced technology ordinarily flowed through to IRGC proxies al-Qaeda and the Taliban. That banned technology was crucial to perpetrate terrorism. By way of example, terrorists were able to use cell phones and other telecommunication technology and software to perpetrate attacks on Americans.

639. ZTE also assisted the terrorist enterprise by serving as a long-term strategic partner for MTN Irancell, which was a front for Hezbollah, the Qods Force, and Regular IRGC.

640. It would be improper to characterize ZTE's role as only modernizing Iran's cellular and communications systems or providing cellular and landline telecommunications infrastructure for use by the Iranian population. On top of the millions of dollars that ZTE provided to the IRGC (including Hezbollah and the Qods Force) via TCI, ZTE also provided technical aid to the IRGC (including Hezbollah and the Qods Force) which facilitated terrorism. ZTE's, ZTE USA's, and ZTE TX's (after its formation) technology transfers were devastating to America's ability to protect Americans overseas from attacks committed by Iranian terrorist proxies like Hezbollah. This was because, as a result of their actions, "[t]he IRGC will also [was] a position to benefit from sensitive monitoring technology it can put to its advantage to enhance its surveillance abilities," which Hezbollah, the Qods Force, and Regular IRGC acquired after "ZTE Corporation sold TCI a powerful surveillance system capable of monitoring landline,

mobile and internet communications.”²³⁷ ZTE’s, ZTE USA’s, and ZTE TX’s (after its formation) technology transfer uniquely provided terrorists the ability to intimidate and coerce civilian populations.

641. For example, according to U.S. diplomatic cables and statements by Lebanese government officials, TCI and the Qods Force helped build Hezbollah’s fiber optic communication system, which was upgraded to include encrypted high-speed lines, and included, according to public reports and on information and belief, Defendants’ “Western technology.” This communication network facilitated intelligence collection and operations in Iraq, and helped Hezbollah defend against US intelligence collection. Hezbollah officials said that this network was their most valuable weapons system.²³⁸ TCI’s work in Lebanon, incorporating technology illegally smuggled by Defendants, enabled Hezbollah, the Qods Force, and Regular IRGC to fully integrate Hezbollah into its transnational command, control, communications, computing, intelligence, surveillance, and reconnaissance apparatus.²³⁹

642. Further, Iranian cellular networks, administered by ZTE and Huawei (for MTN), were also used to track and target U.S. forces in Afghanistan and Iraq. Because they included US technology, they could be used to locate U.S. forces with precision. U.S. soldiers close to the Iranian border would get continuously pinged by Iranian cell phone towers. The “ZXMT” monitoring system that ZTE sold to Iran (with U.S.-origin components) could use this data to triangulate their positions and monitor their communications. Hezbollah, the Qods Force, and

²³⁷ Dr. Ottolenghi Sept. 17, 2015 Testimony.

²³⁸ Liz Sly, Lebanon's fiber-optic powder keg; Iran’s hand seen in Hezbollah's growing communication grid, amid fears of 'state within a state,' *Chicago Tribune*, May 16, 2008.

²³⁹ Carl Anthony Wege, “Hizbollah–Syrian Intelligence Affairs: A Marriage of Convenience,” *Journal of Strategic Security*, Volume 4, Issue 3, 2011.

Regular IRGC also continuously upgraded Hezbollah's communications systems, enabling them to deploy cellular phone systems securely and thwarting U.S. efforts to collect intelligence on their operations.²⁴⁰

643. For a terrorist group intent on targeting Americans traveling in tightly secured convoys or on heavily fortified bases, the technology that ZTE (via, on information and belief ZTE USA and ZTE TX) provided bolstered the terrorists' ability to conduct successful surveillance. The technology ZTE provided was vitally important to their ability to execute successful attacks, like the ones that killed and injured Plaintiffs and their loved ones. For these reasons, ZTE's acts, which allowed terrorists access to modern telecommunications technology they could not otherwise obtain, facilitated intimidation, coercion, and violent acts and acts dangerous to human life.

644. The ample evidence of ZTE's own consciousness of guilt supports the inference that ZTE knew it was benefiting the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise.

645. In 2017, the United States Commerce Department disclosed two internal ZTE documents it had discovered during its investigation. The first, from 2011 and signed by several senior ZTE executives, detailed how the company had ongoing projects in Iran. Written by ZTE's general counsel, signed by its senior management, and flagged as "Top Secret," the document described a number of ways in which Defendants ZTE and its U.S. subsidiaries (including ZTE USA) were, in concert, violating U.S. laws well before 2011.²⁴¹ In sum and

²⁴⁰ Colin P. Clarke, "How Hezbollah Came to Dominate Information Warfare," *Jerusalem Post*, September 17, 2017.

²⁴¹ ZTE "Report Regarding Comprehensive Reorganization and the Standardization of the Company Export Control Related Matters (Top Secret Internal Use Only)," August 5, 2011.

substance, it indicates that while high-level managers of ZTE were also directors of ZTE USA, and frequently shuttled between the two countries, their company's U.S. research centers — soon thereafter to be overseen by ZTE TX — were “often” engaged in the illegal transfer of U.S. research data to China. It also indicates that ZTE was illegally exporting US-origin technology as early as 2005, and that ZTE, as well as its officers, knew that they could face both criminal and civil penalties based on their then-existing contracts. The second document laid out detail in a complex flow chart a ZTE's proposed method for circumventing United States export controls and getting U.S.-origin technology to Iran.

646. According to the then-Acting Assistant Attorney General, Mary B. McCord, “ZTE engaged in an elaborate scheme to acquire U.S.-origin items, send the items to Iran and mask its involvement in those exports,” and the plea agreement ZTE signed “alleges that the highest levels of management within the company approved the scheme.”

647. In 2012, after ZTE's original contract with TCI, which allowed the IRGC (including Hezbollah and the Qods Force) to build a country-wide surveillance system capable of monitoring landline, mobile, and internet communications, was widely reported, ZTE claimed it would stop its business with fronts for the IRGC, including its Hezbollah Division and the Qods Force. In or around March 2012, ZTE spokesman David Shu said in a telephone interview “[w]e are going to curtail our business in Iran.” Although that was a lie, because ZTE thereafter doubled-down on its business relationships with Hezbollah, the Qods Force, and Regular IRGC fronts, it was also an admission that such business was fraught with risk that it would support and contribute to terrorism.

648. Ashley Kyle Yablon, ZTE USA's former general counsel, gave the FBI an affidavit in May 2012 in which he alleged ZTE had plotted to cover up the Iran sales. ZTE

employees asked Mr. Yablon, a ZTE USA employee, to help develop a strategy to transfer U.S.-origin goods to sanctioned countries. Yablon has indicated that in the course of the U.S. investigation into ZTE's transfer of U.S.-origin technology to Iran, ZTE internally discussed destroying evidence, and it has been reported that ZTE employees told Mr. Yablon to gather the evidence that he had of the U.S.-origin technology transfers to Iran, which he had in the United States, and Mr. Yablon instructed ZTE USA employees not to destroy evidence regarding ZTE USA's exports relevant to ZTE's agreement to export U.S.-origin goods. After the Yablon affidavit became public in July 2012, ZTE, which otherwise directed his activities in the United States, placed Yablon on administrative leave.

649. ZTE destroyed evidence of its business with fronts for Hezbollah, the Qods Force, and Regular IRGC and, on information and belief, ZTE USA destroyed evidence in the United States of its business with fronts for Hezbollah, the Qods Force, and Regular IRGC.

650. There has been public reporting related to ZTE's internal documentation of its strategies for how to get around export controls so it can do business with state sponsors of terrorism. Those strategies included using a codeword for Iran in internal documents. On information and belief ZTE USA and/or ZTE TX participated in these strategies.

651. Throughout the scheme, ZTE attempted to conceal its export of U.S.-sourced technology to Hezbollah, the Qods Force, and Regular IRGC by, among other things, requiring its employees to sign non-disclosure agreements, lying to its own lawyers regarding its exports, lying to a forensic expert hired to conduct an internal investigation, and adopting a policy and hiring thirteen (13) employees to alter, delete, and hide data relevant to the export sales.

652. ZTE admitted that it assembled and authorized a team of IT employees to engage in a project to alter, process, sanitize, and/or remove references to Iran in ZTE's internal

databases regarding its business with fronts for the IRGC, including its Hezbollah Division and the Qods Force. The IT team coordinated with various relevant divisions throughout the company, including the sales, procurement, and finance divisions, as well as ZTE's subsidiaries in the United States including but not limited to ZTE USA, to locate and remove any references to Iran or ZTE's business with fronts for the IRGC, including its Hezbollah Division and the Qods Force. The employees executing this IT project were instructed to, and did in fact, delete their emails related to the project.

653. ZTE's acts related to its export of U.S. embargoed technology to Iran, and its attempts to hide and obscure the same, were labelled by the United States Government as a "cover-up."

654. In relation to ZTE's acts to export U.S. embargoed technology to Iran, and its attempts to hide and obscure the same, the U.S. Government charged ZTE with making materially false, fictitious, and fraudulent statements and representations to the United States Federal Bureau of Investigation.

655. In 2017, ZTE chairman and chief executive acknowledged guilt for its acts to evade the embargo and provide banned technology and goods to Iran, saying "ZTE acknowledges the mistakes it made, takes responsibility for them and remains committed to positive change in the company."

656. ZTE knew that it was breaking U.S. law when it exported sensitive telecommunications technology to Hezbollah, the Qods Force, and Regular IRGC and knew or recklessly disregarded that the entities with which it was transacting business (and indeed who were receiving that technology) were fronts for Hezbollah, Qods Force, and Regular IRGC

terrorists who were actively attempting to kill Americans by facilitating attacks by al-Qaeda and the Taliban against Americans in Afghanistan.

657. From 2008 through at least 2016, ZTE's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC, which flowed to al-Qaeda and the Taliban and was used to attack Americans in Afghanistan, including Plaintiffs and their loved ones.

ii. ZTE Corp., ZTE USA, And ZTE TX Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies

658. ZTE Corp.'s ZTE USA's, and ZTE TX's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI (including MCI), Exit40, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to, among others, Hezbollah, the Qods Force, and Regular IRGC, which flowed through to al-Qaeda and the Taliban and facilitated attacks against Americans in Afghanistan, including Plaintiffs.

659. ZTE Corp., ZTE USA, and ZTE TX significantly increased the cash flowing through MTN Irancell and TCI, and ultimately being deployed by Hezbollah, the Qods Force, and Regular IRGC. They did so by illicitly supplying the state-of-the-art American technologies, like servers, to MTN Irancell and TCI, and by extension the IRGC (including Hezbollah and the Qods Force) needed to attack Americans abroad.

iii. ZTE Corp., ZTE USA, And ZTE TX Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies

660. ZTE Corp. has engaged in serial bribery around the world to win business including large 6- and 7-figure bribes. According to a report published by a team of

investigators hired by a hedge fund, “ZTE has engaged in systemic, centrally managed corruption at a scale rarely seen in international commerce.”²⁴²

661. On at least two prior occasions, the same ZTE Corp. leadership team here bribed foreign officials in procurement settings that were like MTN Irancell (other than being in a different geography). ZTE Corp. paid nearly \$800,000 to one decision-maker, more than \$1 million to a second, and \$10 million to a third (all serving in different countries).²⁴³

662. On March 13, 2020, NBC News reported that “ZTE” was “the subject of a new and separate bribery investigation by the Justice Department,” under the Foreign Corrupt Practices Act (“FCPA”). The investigation “center[ed] on possible bribes ZTE paid to foreign officials to gain advantages in its worldwide operations.”²⁴⁴

663. The Justice Department’s current FCPA investigation concerning ZTE Corp. involves ZTE Corp.’s conduct within the United States.²⁴⁵

664. ZTE is not a “normal” multinational corporation but rather, a notoriously dirty company that seeks to advance the agenda of the Chinese Communist Party. It is willing to

²⁴² Bill Gertz, *Report Urges U.S. Action Against Chinese Telecom Giant ZTE Over Corruption Record*, Wash. Times (Dec. 10, 2020) (“Gertz, *Report Urges U.S. Action*”).

²⁴³ Don Woolford, *Somare, The Controversial Father of PNG*, AAP Newswire (Febr. 25, 2021) (“[Michael Somare] faced various claims of impropriety or worse, including being given a \$780,000 bribe by Chinese phone giant ZTE. He was found guilty of submitting late and incomplete financial statements.”).

²⁴⁴ Gretchen Morgenson and Tom Winter, *The U.S. Is Now investigating Chinese Telecom Giant ZTE For Alleged Bribery*, NBC News (Mar. 13, 2020) (“Morgenson and Winter, U.S. Is Now Investigating”).

²⁴⁵ This is necessarily true because, as the *Wall Street Journal* reported, “[t]he U.S. usually doesn’t have jurisdiction to enforce the FCPA against foreign companies lacking securities that trade in the U.S., but can investigate such cases if actions took place within its borders, or if money used in the alleged scheme was wired through the nation’s financial system.” Aruna Viswanatha and Corinne Ramey, *U.S. Probes Chinese Telecom Giant ZTE for Possible Bribery; The Justice Department Investigation Comes After The Company Already Pleaded Guilty To Dodging U.S. Sanctions On Iran*, Wall Street Journal (Mar. 13, 2020).

engage in corrupt deals that most other corporations shun. For example, NBC News (citing a Norges Bank Council on Ethics report) noted that “Norway’s giant government pension fund banned ZTE from its investment universe” in 2016 “based on ‘the risk of severe corruption.’”²⁴⁶ As *NBC News* stated, “[o]nly **three other companies** are barred by the Norwegians for ‘gross corruption’ alongside ZTE.”²⁴⁷

665. ZTE Corp. has pursued an integrated global sales strategy, under which one may infer that ZTE Corp. followed the same, or a substantially similar, bribery tradecraft with respect to similar “pitches” for other state-owned telecom companies.

666. Plaintiffs’ allegations comport with ZTE Corp.’s kickback schemes in other similarly situated governments, e.g., the Philippines, where ZTE Corp. paid millions in bribes.²⁴⁸

667. Audrye Wong is an Assistant Professor of Political Science and International Relations at USC and a Wilson Center China Fellow. In 2021, Ms. Wong published a detailed analysis of Chinese economic tradecraft including, among other things, the Chinese Communist Party’s heavy emphasis on bribery as a matter of policy:

But perhaps ***the most prominent feature of China’s economic statecraft*** is its use of ***positive inducements***. These incentives come in two forms: under the table, whereby Beijing buys off political leaders through illicit deals, and by the book. ... China often provides economic inducements in illicit and opaque ways ... As

²⁴⁶ *Id.*

²⁴⁷ *Id.*

²⁴⁸ “Chinese subversion has not worked as well in countries with greater transparency and oversight. Take the Philippines during the presidency of Gloria Arroyo, ... Costs for a national broadband network, to be built by the Chinese state-owned company ZTE, skyrocketed by \$130 million to \$329 million ***because of kickbacks to key political players***, including the chair of the Philippines’ electoral commission and the president’s husband. As if on cue, in 2005, the Philippines’ national oil company signed an undersea resource exploration agreement that legitimized China’s maritime claims. Audrye Wong, *How Not to Win Allies and Influence Geopolitics: China’s Self-Defeating Economic Statecraft*, Foreign Affairs, Volume 100; Issue 3 (May 1, 2021), (emphasis added), 2021 WLNR 15954005.

Chinese companies have increasingly invested overseas, state-owned enterprises or private companies, sometimes with the tacit approval of Chinese officials, have offered bribes and kickbacks to elites in countries receiving investment or aid projects in order to grease the wheels of bureaucracy. At other times, Chinese companies have bypassed the process of competitive bidding and regulatory approval to secure a contract, often at inflated costs, generating extra profits for both Chinese actors and local elites. I call such inducements "subversive carrots." In many ways, their use reflects China's domestic political economy, where businesses depend on official connections, corruption is widespread, and few regulations govern foreign investment and foreign aid. My research shows that this method works *best* in countries that also have *little public accountability*—where the flow of information is restricted, and political leaders need not worry about public opinion and the rule of law.²⁴⁹

668. On information and belief, from 2010 through 2016, ZTE Corp. caused the payment of at least several million dollars, denominated in U.S. Dollars, to one or more officers, agents, or directors of MTN Irancell, TCI, and/or MCI. This money flowed through to fund and arm the IRGC's Shiite Terrorist Proxies and the IRGC's Sunni Terrorist Proxies to support their attacks against Americans around the world.

3. ZTE Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban's, Including The Haqqani Network's, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq

669. ZTE operated lucrative businesses in post-invasion Afghanistan by servicing a broad array of customers there. To increase their profit margins by redirecting attacks away from their business interests – and to intentionally assist the Taliban's effort to drive Americans out of Afghanistan – ZTE knowingly paid protection money to the Taliban, including its Haqqani Network. When ZTE did so, ZTE knowingly assumed a financial, logistical, and operational role in the Taliban's, including the Haqqani Network's, terrorist enterprise in Afghanistan and

²⁴⁹ Audrye Wong, *How Not to Win Allies and Influence Geopolitics: China's Self-Defeating Economic Statecraft*, Foreign Affairs, Volume 100; Issue 3 (May 1, 2021), (emphasis added), 2021 WLNR 15954005.

beyond by directly and indirectly routing protection payments to these terrorists in cash and “free goods,” including secure American cell phones.

670. ZTE has become one of the world’s most valuable communications technology manufacturers by providing a comprehensive suite of communications technologies services to customers in high-risk geographies from a counter-terrorism perspective, including geographies where Hezbollah, the Qods Force, and Regular IRGC and IRGC proxies al-Qaeda and the Taliban, including its Haqqani Network, raised and moved money to facilitate terrorist attacks through protection payments, procurement corruption, “free goods” payoffs, payments routed through consultants, and similar schemes that depended upon complicit corporate partners.

671. ZTE followed that model in Afghanistan, where ZTE has continuously operated for decades.

672. From 2006 through 2019, ZTE sold products to Afghan telecommunications operators, e.g., MTN Afghanistan, which was MTN’s subsidiary in Afghanistan, which were manufactured by the ZTE Defendants.

673. While ZTE was achieving rapid growth in Afghanistan, the communications sector provided a critical source of financing for the Taliban, including its Haqqani Network, in the same manner as it did for Defendant Huawei and co-Conspirator MTN. ZTE’s payments mirrored the protection money delivered by Huawei and co-conspirator MTN. Just as the Taliban raised “taxes” from international contractors doing business in Afghanistan, so too did it levy similar “taxes” on “the big telecom companies” like ZTE.²⁵⁰

²⁵⁰ *Ruttig, The Other Side* at 20.

674. ZTE's services in Afghanistan required ZTE work in geographies that were controlled or contested by the Taliban, including its Haqqani Network, in which ZTE paid protection payments as a cost of doing business.

675. ZTE's sales to its Afghan customers depended upon ZTE personnel successfully being able to drive large truck convoys containing ZTE's lucrative Afghan-customer-bound goods through Taliban, including Haqqani Network, controlled or contested geographies in Pakistan and Afghanistan.

676. ZTE paid the money as protection: ZTE decided that the cheapest way to shield their projects from attack was to pay the Taliban, including its Haqqani Network to leave them alone and instead attack other targets – like Plaintiffs and their family members. Similar payments were pervasive throughout Afghanistan and supplied the Taliban with an important stream of financing to fund their terrorist attacks across the country.

677. The Taliban, including its Haqqani Network, conveyed its protection-money demands to ZTE via Night Letters similar the ones the Taliban sent to MTN and Huawei.

678. ZTE was a particularly aggressive practitioner of protection payments. Rather than invest in expensive security for shipments, ZTE purchased cheaper “security” by buying it from the Taliban, including its post-FTO-designation Haqqani Network.

679. ZTE negotiated its protection payments in direct discussions between ZTE Afghanistan's security department and Taliban, including Haqqani Network, commanders.

680. Like other contractors in Afghanistan, ZTE generally paid, as protection to the Taliban (including its Haqqani Network), at least ten percent (10%) of its contract budget – and, on information and belief, much more than this – on any contract in which ZTE, including any

ZTE affiliate or contractor, provided services to any customer in Afghanistan, since the Taliban controlled or contested every geography in which ZTE worked.

681. ZTE's practice of making protection payments to the Taliban extended to the Haqqani Network. From at least 2008 through 2017, ZTE operated infrastructure projects sites, and/or sold communications technology products to customers (and therefore transported lucrative commodities through territory) in Afghanistan that was controlled by the Taliban, including its Haqqani Network, and ZTE purchased security for those project sites and shipments by paying the Taliban, including its Haqqani Network. The Haqqani Network's chief financial operative, Nasiruddin Haqqani, oversaw those payments, and they typically occurred on a semi-annual basis, and the Haqqani Network's overall involvement in the scheme was ultimately supervised by Sirajuddin Haqqani, who was at all times a dual-hatted al-Qaeda/Taliban terrorist.

682. ZTE Corporation keyed ZTE's rapid growth in Afghanistan by sponsoring a vast stream of payoffs to the Haqqani Network from 2006 through today, which flowed through to benefit al-Qaeda and the entire Taliban. Under Sirajuddin Haqqani's leadership, as executed by his immediate family members, the Haqqani Network was responsible for collecting "taxes" from Afghanistan's telecom companies, which were the single largest (legal) industry and tax base in Afghanistan – and thus a key source of funding and power for the Taliban and al-Qaeda, both of which were effectively led by Sirajuddin Haqqani in Afghanistan and Pakistan.

683. The logic behind ZTE's payoffs to the Haqqani Network matched the logic motivating ZTE's joint venture with the IRGC. ZTE's leadership intended to harm American interests in Afghanistan (like Iraq), and supporting the Taliban allowed them to do so. ZTE's decision to route monthly protection payments to al-Qaeda (via Sirajuddin Haqqani and his immediate family members) and the Taliban or face the risk that terrorists commanded by

Sirajuddin Haqqani would destroy some of ZTE's shipments. Ordinarily, the going protection payment rate was usually around \$500 to \$2,000 per truck per convoy. In some areas, ZTE caused payments to be made to local Taliban, including Haqqani Network, commanders. In other places, where ZTE operated in a Taliban-controlled environment, the payments would have to be sent to the Taliban's Quetta Shura for southern Afghanistan, e.g., Helmand, or the Taliban's Miram Shah Shura for eastern Afghanistan, e.g., Paktia (Sirajuddin was involved in the former and led the latter).

684. By 2006, the Taliban, including its Haqqani Network, prized the acquisition of western communications technologies, including American-made cell phones, that were "washed" through the IRGC or one of its corporate partners, like ZTE.

685. From 2006 through 2021, ZTE also made protection payments to the Taliban, including its Haqqani Network, in the form of "free goods" – in particular, free communications technologies like cell phones – as an alternative to paying the terrorists in cash. When ZTE did so, ZTE directly provided to the Taliban, including its Haqqani Network, a broad range of communications technologies including, but not limited to, American mobile phones such as American-made Motorola phones, which ZTE reached into the U.S. to specifically acquire for the purpose of transferring such technologies to the IRGC and its proxies, including the Taliban and its Haqqani Network.

686. On information and belief, ZTE transferred millions of U.S. Dollars' worth of American communications technologies, including more than a thousand (1,000) "free goods" black market American-made cell phones to the Taliban, including its Haqqani Network, which ZTE acquired from the United States and delivered to the Taliban, including its Haqqani Network, each year from 2006 through 2021.

687. ZTE’s transfer of free, and illicitly sourced, communications technologies, including technologies that ZTE sourced from the United States, as a means to bribe the Taliban, including its Haqqani Network, comports with ZTE’s long-standing embrace of “free goods” as a core, decades-long, global strategy to route bribes to recipients.

688. U.S. military and intelligence officials have publicly confirmed Plaintiffs’ allegations against ZTE. For example, on June 8, 2012, *Business Insider* confirmed – citing American “military sources” and “former and current intelligence sources” – that that “China [was] likely to remain an aggressive and capable collector of sensitive U.S. economic information and technologies.”²⁵¹ Thus, “[a]nother concern raised by [U.S. military] sources [was] that Huawei and the other Chinese telecommunications companies [i.e., ZTE] also provide[d] technology to Iran and the Taliban.”²⁵²

689. When ZTE provided free communications technologies to the Taliban, including black-market American cell phones, ZTE provided the terrorists a cash equivalent that sponsored tremendous violence. At a going rate of \$2,000 per black market cell phone, for example, the value of ZTE’s illicit phones supplied to the Taliban, including its Haqqani Network, delivered at least \$2 million per year in value to the Taliban, including its Haqqani Network.

690. When ZTE acquired and transferred free communications technologies to the Taliban, including black-market American cell phones, from the United States and delivered such technologies to the Taliban, including its Haqqani Network, ZTE provided devastating operational and logistical assistance to the Syndicate in addition to the financial value of such

²⁵¹ *Business Insider, Military Sources: China Could Shut Down All The Telecommunications Technology It Sold To America* (June 8, 2012).

²⁵² *Id.*

goods through the same operational and logistical benefits that such black-market communications technologies, including American cell phones, accorded to terrorists worldwide.

691. ZTE also directly aided al-Qaeda when ZTE transferred cash and free goods, including the above-described communications technologies and black-market American cell phones, to the Haqqani Network because Sirajuddin Haqqani and his immediate family members, who were responsible for collecting protection payments from telecom companies like ZTE, were also members of al-Qaeda, and thus ZTE funded and logistically supplied al-Qaeda when ZTE routed cash and free goods protection payments to the Haqqani family.

692. ZTE's overall payments to the Taliban, including its Haqqani Network, reached millions of dollars in value in cash and "free goods" payments of communications technologies, including black-market American cell phones each year from 2006 through the present. At that rate, the ZTE Defendants caused at least tens of millions in U.S. Dollar-value in cash and "free goods" to flow through to the Taliban, including its Haqqani Network, from 2006 through the present, which furthered the IRGC's conspiracy to attack Americans in Afghanistan and directly aided the IRGC proxies who committed such attacks, i.e., al-Qaeda and the Taliban, including its Haqqani Network, through attacks committed by joint al-Qaeda/Taliban cells and/or attacks committed by the Taliban that were planned and authorized by al-Qaeda.

4. ZTE's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Including Its Haqqani Network, Comports With ZTE's Historical Sales Practices In International Markets

693. Like MTN, ZTE's conduct reflected a willingness to support America's enemies, and engage in illicit financial transactions, as a way to increase profits in Iran. The same calculation pervaded ZTE's other conduct throughout the world. ZTE's other conduct further demonstrates its pattern and practice of transacting with violent actors to increase ZTE revenue.

694. ZTE has been called a “poster child” for sales of Chinese made network equipment at low prices that “allow the Chinese government to eavesdrop on all communications running on their equipment.”²⁵³

695. Like Iran, North Korea is a designated state sponsor of terrorism with a long history of attacking and murdering Americans overseas. ZTE’s illicit transactions concerning North Korea, therefore, further inform ZTE’s deliberate support for terror.

696. ZTE had a long-term relationship with North Korea. A 2020 civil forfeiture action revealed that — based on ZTE’s disclosures to the U.S. government — it had dedicated account executives and a physical presence in North Korea no later than 2005 and 2007, respectively. ZTE tasked its North Korea account manager with creating two shell companies, one of which received North Korean payments in dollars, and the other of which transferred the money — often using the U.S. financial system — to ZTE. The value of the goods smuggled this way exceeded \$300 million. During this time, North Korea had an extensive relationship with Hezbollah, the Qods Force, and Regular IRGC and Hezbollah. One Court found this support included providing military hardware and training, most notably training for senior leaders and Hezbollah’s intelligence cadre. Thereby, North Korea provided material support to Hezbollah, including but not limited to in relation to the illicit technology transferred to North Korea by ZTE.

697. As part of its guilty plea, “ZTE ... pleaded guilty ... to violating U.S. sanctions against Iran and North Korea.”²⁵⁴ Like with Iran, when it helped North Korea source embargoed

²⁵³ Gertz, *Report Urges U.S. Action*.

²⁵⁴ Gretchen Morgenson and Tom Winter, *The U.S. Is Now investigating Chinese Telecom Giant ZTE For Alleged Bribery*, NBC News (Mar. 13, 2020) (“Morgenson and Winter, *U.S. Is Now Investigating*”).

goods, ZTE knew or recklessly disregarded that it was engaging in illicit transactions with North Korean counterparties in violation of U.S. and international sanctions that were designed to choke off North Korea's support for terrorism. Moreover, even after ZTE got caught helping North Korea evade U.S. sanctions (and pledged to be truthful with the U.S. government), ZTE lied and made additional false statements to American authorities.²⁵⁵

698. As legal commentator Stewart Baker noted at the time in 2012, when discussing ZTE's corporate criminal culture, that "[a] kind of perfect storm has struck ZTE, ... [a] storm largely of ZTE's own making."²⁵⁶ He explained:

ZTE ... ha[s] been the subject[] of great national security concern for years. ... Now, though, the mess is everywhere, and the House intelligence investigation will surely be heavily influenced by the new evidence that ZTE at least is quite capable of ***carrying out sophisticated telecommunications surveillance, of violating US law, and perhaps even lying about it later.*** Which, come to think of it, is pretty much what US intelligence agencies have been saying all along.²⁵⁷

699. Plaintiffs' allegations concerning ZTE's willingness to pay bribes and protection payments, in cash and free goods, are also consistent with ZTE's recent history, as documented

²⁵⁵ As *NBC News* noted, "[i]n the deal with the U.S. government [in 2017], ZTE also agreed to a denial of export privileges that could be activated for seven years if the company committed additional violations. In mid-April 2018, the Commerce Department activated the denial of privileges after determining that ZTE had made false statements to the government about actions it had taken to punish employees involved in the Iran and North Korea activities. While ZTE said it had reprimanded the employees, the government later found that the company had rewarded them with bonuses. Activating the denial meant that ZTE could not buy semiconductors required for its products." *Id.*

²⁵⁶ Stewart Baker, *And You Think You're Having A Bad Day?*, *The Volokh Conspiracy* (July 13, 2012) (emphasis added), 2012 WLNR 14621514.

²⁵⁷ *Id.*

by press reports concerning allegations of “rampant corruption” and programmatic bribery by ZTE around the world for decades.²⁵⁸

5. ZTE’s Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Including Its Haqqani Network, Had A Substantial Nexus To The United States

700. ZTE’s assistance to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied on significant contacts with the United States. As it has admitted, ZTE orchestrated both those U.S. contacts and ZTE’s violation of U.S. law, including, on information and belief, by and through coordination with ZTE USA and ZTE TX. Like MTN, ZTE employs a top-down management structure in which ZTE centralizes operational control over the functions performed by its various subsidiaries.

701. ZTE’s decision to assist Hezbollah, the Qods Force, and Regular IRGC and by extension their proxies, al-Qaeda and the Taliban, had a substantial nexus to the United States for the reasons explained below.

i. ZTE’s Conduct Targeted the United States

702. ZTE’s provision of material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, was expressly aimed at the United States. At all relevant times, ZTE knew that Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, were targeting the United States. Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani

²⁵⁸ See, e.g., Gertz, *Report Urges U.S. Action* (“Chinese telecommunications company ZTE has been involved in international bribery incidents around the world but so far escaped prosecution by the Justice Department for corrupt practices... according to a report... based on court documents, interviews with prosecutors, and news reports showing ZTE linked to corrupt practices in more than a dozen countries....”).

Network, did not conduct an indiscriminate terrorist campaign that merely injured Americans by chance. Instead, Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, directed attacks at *Americans* with the specific intent of killing *Americans* in particular – so that they could inflict pain in the United States and influence U.S. policy. As the Treasury Department stated when it announced the Qods Force’s designation as a SDGT in 2007, “the Qods Force provides lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi’a militants who target and kill Coalition ... forces...”²⁵⁹ Hezbollah’s, the Qods Force’s, Regular IRGC’s, al-Qaeda’s, and the Taliban’s, including its Haqqani Network’s, ultimate, shared, publicly stated goal was to effect a withdrawal of American forces from Afghanistan and the broader Middle East. Each terrorist attack that killed and injured Plaintiffs was part of that campaign of anti-American terrorism.

703. ZTE’s decision to reach into the United States, including by coordinating with ZTE USA and ZTE TX, to obtain embargoed dual-use technology to aid the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist enterprise was also expressly aimed at the United States. Like MTN, ZTE knew, based on conversations with IRGC, including Hezbollah and the Qods Force, agents, that Hezbollah, the Qods Force, and Regular IRGC viewed ZTE’s assistance as vital to Iranian national “security,” which ZTE understood to inherently involve the promotion of terrorist violence against Americans around the world as part of Hezbollah’s, the Qods Force’s, and Regular IRGC’s effort to export its Islamic Revolution and drive the U.S. out of Afghanistan.

²⁵⁹ U.S. Treasury Dep’t, *Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007).

704. On information and belief, like MTN, ZTE also knew, based on conversations with U.S. officials, that it was assuming an active role in a Hezbollah, the Qods Force, and Regular IRGC plot to develop cash flow and source vital dual-use components for the Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network. ZTE further knew of the critical importance that communications and computing technology plays for terrorists.

705. When ZTE, ZTE USA, and ZTE TX sourced embargoed technology, including by coordinating with ZTE USA and ZTE TX, that the United States had publicly declared could benefit IRGC, including Hezbollah and the Qods Force, efforts to kill others, they intentionally helped arm terrorists they knew were targeting the United States. On information and belief, Hezbollah, the Qods Force, and Regular IRGC made ZTE agree to a similar contractual pledge as the one in which MTN agreed to aid Iran's "defensive, security, and political" interests outside of Iran. On information and belief, at all times, ZTE knew or recklessly disregarded that "security" was a euphemism for IRGC, including Hezbollah and the Qods Force, terrorist operations outside of the territorial borders of Iran. When ZTE, ZTE USA, and ZTE TX obtained the technology requested by its IRGC, including Hezbollah and the Qods Force, partners, each took actions in the United States and targeted at United States by helping the terrorists improve their bombs, rockets, communications, and intelligence gathering.

706. Although ZTE's primary motivation for assisting Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and Taliban was financial, ZTE also intended to harm Americans in Afghanistan. One reason ZTE cooperated with Hezbollah, the Qods Force, and Regular IRGC was to align itself with their effort to drive Americans out of Afghanistan.

707. Like MTN, ZTE intended to harm Americans because it decided that was the necessary price of maintaining a good relationship with Hezbollah, the Qods Force, and Regular IRGC who were explicit, that they expected their partners to provide significant help in fighting against U.S. forces in particular. Thus, for ZTE to achieve its business objectives vis-à-vis Hezbollah, the Qods Force, and Regular IRGC fronts who controlled TCI and MTN Irancell – both of which ZTE serviced – ZTE needed to disassociate itself from the United States and prove that it could deliver value to the Shiite terrorist campaign against U.S. forces in Iraq.

708. On information and belief, like MTN, ZTE’s agreement to aid Hezbollah, the Qods Force, and Regular IRGC also fulfilled an obligation by ZTE, like MTN, to engage in “defensive, security and political cooperation” with its IRGC, including Hezbollah and Qods Force, counterparties.²⁶⁰

709. Indeed, ZTE’s contract with TCI, according to Yablon, obligated ZTE to transfer its U.S.-built surveillance systems to TCI. When *Reuters* revealed that the ZXMT system contained U.S.-origin components, the Department of Commerce, BIS, served ZTE USA with an administrative subpoena and the U.S. Attorney’s office for the Northern District of Texas opened its grand jury investigation and the FBI served ZTE USA with criminal subpoenas.

710. The “surveillance function” built into ZTE’s contract, on information and belief, obligated ZTE to collaborate with Iranian ‘security’ authorities, including, *inter alia*, IRGC entities that implemented the regime’s campaign of terrorism.

711. Thereby ZTE, along with IRGC-controlled TCI, are responsible for helping the IRGC collect signals intelligence within Iran. According to the U.S. government, the IRGC

²⁶⁰ Exhibit A, MTN-Irancell Consortium Letter Agreement § 8.

Committee to Determine Instances of Criminal Content identifies websites, which TCI blocks and monitors.

712. In their campaign of mass repression, these IRGC, including Hezbollah and the Qods Force, agencies rely on technology illegally supplied by the Defendants, and, to justify their actions, a law which criminalizes any effort to evade the IRGC's censorship, creating online "groups or gatherings" that threaten the state, or linking to sites connected to "wayward and illegal groups and movements" as "creating content against national security."²⁶¹

713. *First*, ZTE's support for Hezbollah, the Qods Force, and Regular IRGC did not merely grow ZTE's profits by allowing it to obtain lucrative business from MTN Irancell and TCI in the first instance; it also benefited ZTE's business by inflicting harm on an enemy (the United States) of one of ZTE's most important business partners (Hezbollah, the Qods Force, and Regular IRGC) in order for ZTE to curry Iranian favor to gain market share for a potentially uniquely lucrative telecom and communications market (Iran).

714. *Second*, ZTE's support for attacks against U.S. citizens by Shiite terrorists advanced the foreign-policy interests of ZTE's most important business partner: the Chinese Communist Party (or "CCP").

715. At all relevant times, ZTE has acted as an anti-American Chinese nationalist company that actively seeks to advance the interests of the Chinese Communist Party.

716. ZTE specifically pursued transactions with Qods Force fronts in order to harm the United States in the Middle East as part of a broader Chinese Communist Party strategy to inflict

²⁶¹ Justice for Iran "*Gerdab: a Dictated Scenario*" 2012 p.36 <https://justice4iran.org/wp-content/uploads/2012/03/Gerdab-a-dictated-scenario.pdf>.

pain on America in the Middle East by supporting the Qods Force and its terrorist campaign against Americans there.

717. Indeed, ZTE has pursued this objective continuously since 9/11. For example, less than two weeks after that attack, commentators were already observing ZTE's efforts to curry favor with the Taliban, even though they were understood to have sheltered bin Laden and contributed to the attack as a result. As one wrote at the time:

China ... has been playing its own complex "Great Game," through the Taliban in Afghanistan, and in alliance with Pakistan. ...

One of the great myths about modern, Communist China is that it has no territorial or imperial ambitions. It has them, but does not admit they are imperial, in the western sense.

This modern China still aspires to rule directly over all her immediate neighbours, including Korea, and to exact "tribute" from the countries beyond them. It aspires to be a superpower, on a level with the United States, and has not hesitated to link itself with revolutionary movements ...

The Chinese attitude towards radical "Islamism" is two-faced. Beijing is happy to train and send armed insurgents – separatist terrorists -- to ... sow mischief wherever it can against Western interests. But it is also worried, sometimes to the point of paranoia, about the security threat to its own Uighur territory. ...

From the Beijing point of view, co-operation with the Taliban kills two birds with one stone. On the one hand, China has been helping to nurture a very painful thorn in the West's backside; on the other, it is buying off Taliban encouragement for Uighur separatists. Until Sept. 11, it appeared Beijing's prospects in Kabul were win-win.

By coincidence or otherwise, on Sept. 10, the day before the organized terror assault on New York City and Washington D.C., Chinese representatives in Kabul signed a memorandum of understanding for economic and technical co-operation with Mullah Mohammed Ishaq, the Taliban minister for mining.

It was the most comprehensive of a series of contractual agreements between Beijing and the Taliban, in defiance of the spirit if not the letter of both Western and United Nations sanctions. It confirmed the Chinese role as the Taliban's best friend outside the Islamic world.

The most interesting part of the agreement is a promise to build desperately needed infrastructure for the Taliban regime, throughout the 90 per cent of Afghanistan's surface area now under Taliban control.

Already, last year, two Chinese telecommunications firms, Huawei Technologies and ZTE, began work laying secure land-based phone lines between and within Kabul and Kandahar, and they may well be directly involved in providing communications services to the terrorist "underground" (literally, for it works from caves) in the Kandahar region.

Huawei is the firm that has been installing communications equipment for Iraq's air-defence system. It was named in a protest to the Chinese government by the Bush administration on its first day in office.

The aid to Afghanistan is by no means confined to economy and infrastructure. Political contacts between China and the Taliban have been increasing rapidly. ...

China tries to help the Afghan terrorist regime in its struggle against the West ...²⁶²

718. Faithful to its Chinese Communist Party-supporting trade efforts, ZTE always continued pursuing its nationalistic Chinese agenda. As the legal commentator Stewart Baker noted at the time in 2012, "[a] kind of perfect storm has struck ZTE, ... [a] storm largely of ZTE's own making."²⁶³ He explained:

For starters, ZTE and its larger Chinese rival, Huawei, have been the subjects of great national security concern for years. The US intelligence community fears that, if allowed to install equipment here, the two companies will surreptitiously permit Chinese government wiretaps inside the United States. But proof of this suspicion has been hard to find. And the firms, backed by Chinese government-subsidized loans, have been able to offer enormous discounts to carriers, devastating the global telecom equipment market and leaving carriers eager to buy their products. Whether the US government would continue to act on its suspicions in the face of commercial pressure was an open question. ...

Now, though, the mess is everywhere, and the House intelligence investigation will surely be heavily influenced by the new evidence that ZTE at least is quite

²⁶² David Warren, *How China Advances Its Imperial Ambitions By Backing The Taliban*, Ottawa Citizen (Canada), (Sept. 22, 2001), 2001 WLNR 6660411.

²⁶³ Stewart Baker, *And You Think You're Having A Bad Day?*, The Volokh Conspiracy (July 13, 2012), 2012 WLNR 14621514.

capable of carrying out sophisticated telecommunications surveillance, of violating US law, and perhaps even lying about it later.

Which, come to think of it, is pretty much what US intelligence agencies have been saying all along.²⁶⁴

719. Indeed, ZTE is known to be an “important geopolitical pawn” for the Chinese Government, with direct links to both the Chinese Government and the People’s Liberation Army. It has “substantial ties to the Chinese government and military apparatus.”

720. China's Foreign Ministry confirmed its approval for ZTE’s efforts to undermine U.S. national security when it expressed anger after the U.S. Commerce Department placed export restrictions on ZTE for violating U.S. export controls on Iran. “We hope the U.S. stops this erroneous action and avoids damaging Sino-U.S. trade cooperation and bilateral relations,” Chinese Foreign Ministry spokesman Hong Lei said at a briefing in March 2012.

721. ZTE’s aid for the IRGC and Qods Force are consistent with the Chinese Communist Party’s desire to inflict pain on Americans in Afghanistan. The Chinese Communist Party views the United States being pinned down in conflict in the Middle East, and American being killed or injured in Iraq as beneficial to its interests. This is because protracted conflict in Iraq could give China the ability to expand its influence in the Middle East and could pin down the U.S. military in the Persian Gulf so that it is harder to pivot toward the Pacific.

722. That is why, from the Chinese Communist Party’s perspective, there is strategic value in helping Iran develop enough military capabilities to counter U.S. dominance of the Persian Gulf. Indeed, Wang Jisi, Dean of the Peking University School of International Studies, has argued that the U.S. war with Iraq benefited China because “It is beneficial for our external

²⁶⁴ Stewart Baker, *And You Think You’re Having A Bad Day?*, The Volokh Conspiracy (July 13, 2012), 2012 WLNR 14621514.

environment to have the United States militarily and diplomatically deeply sunk in the Mideast to the extent that it can hardly extricate itself.”

723. Thus, a strong economic, diplomatic, and military partnership with the Islamic Republic could help China offset U.S. power in the Middle East. Similarly, Renmin University professor Shi Yinhong has recently argued that “Washington’s deeper involvement in the Middle East is favorable to Beijing, reducing Washington’s ability to place focused attention and pressure on China.”

724. This year, Iran and China signed an agreement expressing a desire to increase cooperation and trade relations over the next 25 years. It has been reported that this agreement commemorates a shared desire between China and Iran to reduce and resist U.S. influence in the region.

725. ZTE’s agreement to aid Hezbollah, the Qods Force, and Regular IRGC served the Chinese Communist Party’s agenda of inflicting pain on U.S. forces in Iraq. On information and belief, it also fulfilled an obligation by ZTE, similar to that of MTN, to engage in “defensive, security and political cooperation” with its IRGC, including Hezbollah and the Qods Force, partner.²⁶⁵ Such cooperation offered ZTE added motivation for ZTE’s illicit transactions with Hezbollah, the Qods Force, and Regular IRGC. ZTE’s support for Hezbollah, the Qods Force, and Regular IRGC did not merely grow its profits by allowing it to obtain lucrative business from MTN Irancell and TCI in the first instance; it also benefited ZTE’s business by inflicting harm on an enemy of ZTE’s most important business partner (the Chinese Communist Party) and decisionmakers (the IRGC and Qods Force) in a key telecom market (Iran).

²⁶⁵ MTN-Irancell Consortium Letter Agreement § 8 (Sept. 18, 2005).

726. Plaintiffs' allegations also comport with the widespread view of relevant U.S. government officials from the executive and legislative branches. For starters, ZTE was forced to plead guilty and the largest criminal fine, to that date, in a United States sanctions case.

727. Moreover, a group of 33 Senators expressed concern about ZTE. On May 15, 2018, they sent a letter to President Trump indicating they viewed ZTE as a security threat. In relevant part the Democratic Senators (a) noted that ZTE violated US sanctions law and repeatedly lied about steps it would take to remedy the problems; (b) argued that America's national security must not be used as a bargaining chip in trade negotiations; (c) labeled ZTE as a "bad actor"; and (d) argued that loosening restrictions on ZTE could "risk American national security".

728. Concerns about ZTE's hostility to American national security are bipartisan. For example, Senator Marco Rubio has warned against allowing ZTE "to operate in U.S. without tighter restrictions," given national security and espionage concerns, and Senator Mark Warner has publicly reported to label ZTE as a "national security threat."

729. Moreover, a multi-year bipartisan investigation by the House Select Committee on Intelligence concluded in October 2012 that ZTE "cannot be trusted to be free of foreign state influence and thus pose[s] a security threat to the United States and to our systems."

730. Further, the FCC recently designated ZTE as a "national security threat," and stated that "ZTE's violation of U.S. trade agreements and export laws, coupled with its obstruction of the Department of Justice's investigation, indicate a clear disregard for U.S. law and national security." Indeed, the FCC noted that ZTE has broken laws that pertain to U.S. national security, and ZTE has "shown a willingness to obstruct the investigations into such national security threats." The FCC stated concern regarding "ZTE's knowing violations of U.S.

national security laws and its proven lack of cooperation in dealing with U.S. criminal investigators.”

731. OFAC, as well as the other U.S. government agencies, opened an investigation of ZTE in March 2012. As agreed by ZTE in its Settlement Agreement with OFAC, at or around that time, “an undisclosed person in ZTE’s legal department in Shenzhen called at least one ZTE employee present within the United States to instruct him to leave the country. These instructions were provided on the same day or shortly after search warrants were executed upon ZTE’s facilities located in the United States.” On information and belief, these statements relate to actions taken by employees of ZTE’s subsidiaries in the United States, including by not limited to ZTE USA.

732. As part of ZTE’s attempt to “cover up” its acts to provide U.S.-origin technology to TCI, ZTE and ZTE USA retaliated in the United States against the ZTE USA whistleblower in the United States who reported the scheme. ZTE also coordinated with ZTE USA in the United States and used ZTE USA as ZTE’s agent and instrumentality through which ZTE hired legal representation in the United States to respond to United States criminal investigations.

ii. ZTE’s Conduct Relied on American Contacts

733. ZTE reached into the United States to acquire U.S.-sourced embargoed technology that it then provided to Telecommunication Company of Iran and Aryacell.

734. TCI is predominantly state-controlled. Indeed, TCI is owned by the Iranian government and a private consortium with reported ties to IRGC, including Hezbollah and the Qods Force.

735. Aryacell is part of the consortium that, along with Hezbollah, the Qods Force, and Regular IRGC controls TCI.

736. ZTE, including but not limited to in coordination with ZTE USA and ZTE TX, reached into the United States to support Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, when it obtained technology and vital operational support from the U.S. ZTE supplied technology and operational support for TCI and MTN Irancell through various U.S. agents, including but not limited to ZTE USA and ZTE TX. In doing so, ZTE tied its unlawful conduct to the United States by obtaining irreplaceable, best-in-class, and embargoed U.S.-supplied dual-use technology to aid the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise. This U.S. contact was closely related to ZTE's, ZTE USA's, and ZTE TX's support for Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network.

737. ZTE relied on U.S.-made materials as components for its smartphones, cell phone systems, and computer networking gear. U.S.-origin goods were technically essential to ZTE's IRGC-related, including its Hezbollah Division-related and Qods Force-related, projects and/or end-users as there were no suitable foreign-made substitutes for many of them.

738. The embargoed United States technology included but was not limited to servers, switches, routers, and component parts of cellular network infrastructure.

739. The United States Commerce Department has said that ZTE sold prohibited American electronics to Iran to help Iran build its telecom networks.

740. Just about every product that ZTE makes has some American components or software in it, such as microchips, modems, and Google's Android operating system.

741. Public reports indicate ZTE helped funnel software and hardware from U.S. firms including Oracle, Microsoft, and Cisco Systems to the government of Iran in 2010 for use building what was described as a massive, nationwide surveillance system.

742. Simply put, ZTE could not do the business it did with Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, and thereby cause the transfer of key technology to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, without reaching into the United States to obtain that technology.

743. ZTE Corporation's regular transfers of communications technologies, including American cell phones, to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied upon American contacts, American transactions, American persons, and American service providers, and depended upon ZTE Corporation reaching into the United States, or causing agents, cut-outs, or affiliates to reach into the United States, in order to source the premium brand cell phones craved by al-Qaeda and the Taliban at all times after 9/11. On information and belief, from 2005 through present, ZTE Corporation regularly reached into the United States to acquire iconic American communication technologies for the Taliban's benefit, including, but not limited to, numerous technological generations, e.g., iPhone 5, iPhone 6, of: (i) Apple's iPhone and iPad, from California, which were among the most popular cell phones in the Middle East after 2008; (ii) Motorola's Two-Way Push-to-Talk Cell Phone, from Illinois, which was widely associated with Hezbollah and its proxies in the Middle East after the broad media coverage of their use during Hezbollah's 2006 attack campaign against Israel; and (iii) Motorola's Razr Cell Phone, from Illinois, which was one of the most popular cell phones in the Middle East before and after the iPhone.

C. The Huawei Defendants

1. Huawei Joined The Terrorist Conspiracy

i. Through Agreements With Hezbollah, Qods Force, And Regular IRGC Fronts, Including But Not Limited to TCI And Exit40, Huawei Agreed To Join A Company-Wide Conspiracy

744. Huawei and its subsidiaries—including Huawei USA, Huawei Device USA, Futurewei, and Skycom—entered into the conspiracy with Hezbollah, the Qods Force, and Regular IRGC to provide U.S.-origin goods and services, in violation of U.S. sanctions, to TCI and Irancell. The agreement was in the form of contracts that Huawei signed with TCI and, on information and belief, MTN Irancell and MCI. The conspiracy was adopted by Huawei’s senior leadership and deployed throughout Huawei and its subsidiaries (including Huawei USA, Huawei Device USA, Futurewei, and Skycom).

745. On information and belief, Huawei and its subsidiaries, including Huawei USA, Huawei Device USA, Futurewei, and Skycom, entered into a conspiracy to provide U.S.-origin goods and services, in violation of U.S. sanctions, to Exit40. The agreement was in the form of contracts that Huawei signed with Exit40 and, on information and belief, MTN Irancell and MCI. The conspiracy was adopted by Huawei’s senior leadership and deployed throughout Huawei and its subsidiaries, including Huawei USA, Huawei Device USA, Futurewei, and Skycom. Plaintiffs’ belief is based upon MTN Group’s retention of Exit40, which, on information and belief, was for the same purpose and in response to the same IRGC instruction.

746. On information and belief, Huawei’s contracts with its IRGC-front Iranian counterparties all included pledges to assist with the “security” of Iran.

ii. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Each Made Overt Acts In Furtherance Of The Conspiracy

747. Each of the Huawei Defendants, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom, acted in furtherance of the conspiracy by, *inter alia*, (a) sourcing U.S.-origin technology, embargoed by the United States and useful to the terrorists, for export to Hezbollah, the Qods Force, and Regular IRGC (b) entering into contractual relationships with U.S. suppliers to acquire the “essential” technology needed by the terrorists, (c) stealing or otherwise misappropriating U.S.-origin technology and intellectual property from U.S. companies to deliver the same to Hezbollah, the Qods Force, and Regular IRGC (d) developing and using third-party companies to both conceal and facilitate its business with IRGC-front companies, (e) comingling U.S.-origin technology with non-U.S.-origin technology in order to attempt to evade detection of the scheme and conspiracy, (f) providing U.S.-based financial services for its Iranian businesses, (g) lying to U.S. government authorities and financial institutions regarding the nature of their activities in Iran and their true IRGC-front counterparties, (h) destroying evidence related to the scheme and conspiracy, (i) providing the services of a U.S. citizen for its Iranian subsidiary (Skycom) that concealed Huawei’s sourcing of U.S.-origin goods, and (g) moving one or more witnesses in the U.S. with knowledge of the scheme and conspiracy out of the jurisdictional reach of the U.S.

2. Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The IRGC’s, Including its Hezbollah Division’s And Qods Force’s, Terrorist Enterprise Against Americans Worldwide

748. Huawei bid on and secured contracts worth hundreds of millions of dollars to provide telecommunications and network infrastructure equipment and related services in Iran. Huawei knew that its counterparties were IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, operatives, or agents. Huawei developed an elaborate system to fulfill those contracts

using U.S.-origin items and services, which Huawei Co. did in collaboration with and with the assistance of Huawei USA, Huawei Device USA, Futurewei, and Skycom.

i. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Knowingly Facilitated MTN Irancell And TCI Acquisition of Embargoed American Technology, Logistical Support, And Technical Services, Which Flowed Through To The IRGC's Terrorist Proxies

749. Huawei Co.'s, Huawei USA's (after its formation), Huawei Device USA's (after its formation), Futurewei's, and Skycom's company-wide scheme to obtain U.S.-origin goods and to evade export controls to get telecommunications technology into the hands of Hezbollah, the Qods Force, and Regular IRGC lasted from as early as 2008 and as late as 2014. To be clear, although Huawei USA was not formed until at least 2011 and Huawei Device USA was not formed until at least 2010, Plaintiffs allege that Huawei USA, Huawei Device USA, and their employees participated in the scheme to advance the conspiracy after their respective formations.

750. The technology and equipment Huawei sourced from inside the United States was subject to the embargo imposed and enforced by the United States Government. Huawei thus violated export controls designed to keep sensitive American technology out of the hands of Hezbollah, the Qods Force, and Regular IRGC.

751. Through this scheme, which last at least between January 2008 and January 2014, Huawei exported U.S.-origin items to Hezbollah, the Qods Force, and Regular IRGC without obtaining proper export licenses.

752. The Huawei scheme operated in the Eastern District of New York, the Central District of California, the District of Columbia, the District of Delaware, the District of New Jersey, the Eastern District of Texas, the Northern District of California, the Northern District of Illinois, the Northern District of Texas, the Southern District of California, the Southern District

of New York, the Western District of New York, the Western District of Washington and elsewhere, including overseas.

753. To circumvent the U.S. embargo and advance its conspiracy with Hezbollah, the Qods Force, and Regular IRGC Huawei devised a scheme, whereby Huawei would set up subsidiaries disguised as un-related Iranian “partners” and use those subsidiaries to hide Huawei’s business with, and shipment of prohibited U.S. technology to, the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, agents, and operatives. Skycom, which was controlled by Huawei, was one of Huawei’s subsidiaries to serve as an Iranian “partner” in this scheme.

754. After a series of international publications in 2012 publicly revealed Huawei’s sale of prohibited equipment to Iran, Huawei issued statements that denied its involvement in any violations of Iranian sanctions, as well as its ownership and control of Skycom. Despite the media revelations of Huawei’s sanctions-busting scheme, Huawei continued sending U.S.-origin goods and services to the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, agents, and operatives.

755. In 2018, a federal grand jury indictment against Huawei Co., Huawei Device, Huawei Device USA, Futurewei, Skycom, and Wanzhou Meng (“Meng”) in *U.S. v. Huawei Technologies Co., Ltd., et al.* (E.D.N.Y. Case No. 1:18-cr-00457-AMD) (the “Huawei Criminal Case”) was unsealed, revealing numerous criminal charges against the Huawei Defendants relating to their scheme to support Huawei’s global business interests, including its efforts to provide embargoed goods and services to Iran. As detailed in the Superseding Indictment filed on February 13, 2020,²⁶⁶ in the Huawei Criminal Case, Huawei, including its American

²⁶⁶ *U.S. v. Huawei Technologies Co., Ltd., et al.*, No. 18-457 (S-3) (AMD), 2020 WL 1319126 (E.D.N.Y. Feb. 13, 2020).

subsidiaries, including on information and belief Huawei USA, Huawei Device USA, and Futurewei, engaged in a series of unlawful conduct in and/or targeting the United States to carry out its scheme.

756. As part of its international business model, Huawei engaged in business in countries subject to U.S., E.U. and/or U.N. sanctions, including Iran. This business, which included shipping Huawei goods and services to end users in sanctioned countries, was typically conducted through local affiliates in the sanctioned countries, such as Skycom in Iran.

757. Even though the U.S. Department of the Treasury's ITSR, 31 C.F.R. Part 560, proscribed the export of U.S.-origin goods, technology and services to Iran and the Government of Iran, Huawei operated Skycom as an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services, for Huawei's Iran-based business while concealing the link to Huawei. Huawei could thus attempt to claim ignorance with respect to any illegal act committed by Skycom on behalf of Huawei, including violations of the ITSR and other applicable U.S. law, when providing U.S.-origin goods and services to Hezbollah, the Qods Force, and Regular IRGC.

758. At all relevant times, Skycom was owned and/or controlled by Huawei. In her Deferred Prosecution Agreement in the Huawei Criminal Case (dated September 22, 2021), Meng, Huawei Co.'s CFO and Deputy Chairwoman of its Board of Directors, and the daughter of Huawei's founder, admitted that between 2010 and 2014, (a) Huawei Co. controlled Skycom's business operations in Iran, (b) Skycom was owned by Huawei Co., (c) all significant Skycom business decisions were made by Huawei Co., (d) Skycom's country manager (for Iran) was a Huawei Co. employee, and (e) that Huawei's prior public denials of its ownership and control of Skycom was incorrect.

759. Meng was the Secretary of Hua Ying, which is a subsidiary of Huawei Co., when Huawei caused Hua Ying to transfer its Skycom shares to Calicula, which was controlled by Huawei. After the transfer, Meng joined Skycom's Board of Directors, which was comprised of Huawei employees. Meng served on the Skycom Board of Directors until April 2009. After her departure, Skycom's Board members continued to be comprised of Huawei Co. employees. As of August 2012, Huawei included Skycom among a list of "other Huawei subsidiaries" in Huawei Co. corporate documents.

760. Huawei's substantial efforts to circumvent U.S. sanctions and ensure a lucrative stake in the Iranian mobile network market is evidenced by its significant business with the largest (MCI) and second largest (MTN Irancell) Iranian mobile service providers, both of which are controlled by Hezbollah, the Qods Force, and Regular IRGC.

761. The success of MTN Irancell depended on its ability to source critical American technology and equipment for its systems and network, including, but not limited to, equipment from Sun Microsystems Inc., Oracle Corp., International Business Machines Corp., EMC Corp., Hewlett-Packard Co., and Cisco Systems, Inc., that were used to provide such services as wiretapping, voicemail, and text messaging.

762. Huawei, including its U.S. subsidiaries Huawei USA, Huawei Device USA, and Futurewei, leveraged its relationships and contracts with U.S. companies and research and development institutions to access and unlawfully export American equipment and technology through the Skycom scheme.

763. For example, in 2020, Huawei produced internal company records from 2010 evidencing its shipment of Hewlett-Packard equipment, including computer servers and

switches, to MCI via Skycom, contrary to Huawei's prior denials about violating applicable sanctions and its ownership and control over Skycom.

764. At the time this transaction occurred, Huawei had a business relationship with Hewlett-Packard that allowed Huawei to incorporate Hewlett-Packard products into Huawei systems. Huawei took advantage of this arrangement to export surreptitiously embargoed U.S.-origin equipment and technology to Iran. Huawei's conduct was in violation of its distribution contract with Hewlett-Packard, which prohibited the sale of its products into Iran and required compliance with U.S. and other applicable export laws.

765. Huawei's internal company documents confirm that Huawei, including its U.S. subsidiaries Huawei USA, Huawei Device USA, and Futurewei, successfully procured and exported to Iran other U.S.-origin technology as well, including software made by Microsoft Corp, Symantec Corp, and Novell Inc. On information and belief, like it did with Hewlett-Packard, Huawei leveraged its relationships with these American companies to acquire and export U.S.-origin equipment and technology, in violation of its agreements with the American companies and U.S. law.

766. To further Huawei's global business interests, including its desire to export U.S.-origin equipment or technology to MCI and/or MTN Irancell, Huawei, including its U.S. subsidiaries Huawei USA, Huawei Device USA, and Futurewei, misappropriated and/or reverse-engineered US-origin equipment and technology.

767. As revealed by the Department of Justice's investigation, and subsequent indictment of Huawei Co., Huawei Device USA, and Futurewei for racketeering activity, Huawei and its subsidiaries engaged in a decades-long effort to misappropriate intellectual property, including from six U.S. technology companies, in an effort to grow and operate

Huawei's business. The misappropriated intellectual property included trade secret information and copyrighted works, such as source code and user manuals for internet routers, antenna technology and robot testing technology.

768. Huawei, including Huawei USA, Huawei Device USA, Skycom, and Futurewei, and others executed a scheme to operate and grow the worldwide business of Huawei and its parents, global affiliates, and subsidiaries through the deliberate and repeated misappropriation of intellectual property of companies headquartered or with offices in the United States for commercial use.

769. The means and methods of the misappropriation included entering into confidentiality agreements with the owners of the intellectual property and then violating the terms of the agreements by misappropriating the intellectual property for Huawei's own commercial use, recruiting employees of other companies and directing them to misappropriate their former employers' intellectual property, and using proxies such as professors working at research institutions to obtain and provide the technology to Huawei and its subsidiaries.

770. As part of the scheme, Huawei launched a policy instituting a bonus program to reward employees who obtained confidential information from competitors. The policy made clear that Huawei employees, including employees of Huawei USA, Huawei Device USA, and Futurewei, who provided valuable information were to be financially rewarded by Huawei.

771. By misappropriating the intellectual property of the U.S. companies, Huawei received income directly and indirectly, including by benefitting from the sale of products containing stolen intellectual property to Hezbollah, the Qods Force, and Regular IRGC and saving on research and development costs, which income Huawei and its subsidiaries agreed to

use to establish and operate the worldwide business of Huawei and its parents, global affiliates, and subsidiaries, including in the United States and Iran.

772. Huawei, including Huawei USA, Huawei Device USA, Skycom, and Futurewei, agreed to use the proceeds derived from the theft of U.S.-origin intellectual property to establish and operate the business of Huawei and its parents, global affiliates, and subsidiaries in the U.S. and abroad, including Iran.

773. Huawei, including Huawei USA, Huawei Device USA, Skycom, and Futurewei, agreed to benefit from the cost savings generated by stolen intellectual property to innovate more quickly and to establish and operate the business of Huawei and its parents, global affiliates, and subsidiaries in the U.S. and abroad, including Iran.

774. Huawei USA's, Huawei Device USA's, and Futurewei's theft of American technology, trade secrets, and intellectual property under this scheme were directed by, and for the benefit of, Huawei Co. and Huawei's global business interests, including Huawei's agreements with Hezbollah, the Qods Force, and Regular IRGC. For example, as revealed in an investigation conducted by the Permanent Select Committee on Intelligence for the U.S. House of Representatives, several current and former employees of Huawei USA provided information indicating that Huawei USA is managed almost completely by Huawei Co. in China.

775. Huawei Co. controlled and directed each of its American subsidiaries' participation in its scheme to source U.S.-origin goods and services for Hezbollah, the Qods Force, and Regular IRGC and each of its American subsidiaries provided Huawei different channels by which Huawei could obtain or misappropriate U.S.-origin goods and services.

776. According to Huawei's public statements and disclosures, Huawei USA specializes in enterprise and network carrier business, Huawei Device USA focuses on the

consumer business (e.g., handsets and routers), and Futurewei is Huawei's research and development arm. Thus, by directing each of its American subsidiaries to participate in its scheme to source U.S.-origin technology for Hezbollah, the Qods Force, and Regular IRGC Huawei created a comprehensive system for maximizing its procurement and export of U.S.-origin goods and services.

777. Huawei's scheme also included the provision of unlawful financial services to the IRGC's, including Hezbollah's and the Qods Force's, fronts, operatives, and agents.

778. In the Eastern District of New York and elsewhere, Huawei Co. and Skycom, together with others, conspired to cause the export, reexport, sale and supply, directly and indirectly, of banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, C.F.R., Sections 560.203, 560.204 and 560.206.

779. For example, after Huawei's Senior Vice President testified before U.S. Congress on September 13, 2012 that Huawei's business in Iran had not "violated any laws and regulations including sanction-related requirements" and other Huawei officers repeated those misrepresentations to financial institutions, Huawei Co. and Skycom completed the following unlawful financial transactions in America, involving U.S. banks, and/or international financial institutions and their U.S. subsidiaries: \$52,791.08 U.S.-dollar clearing transaction on July 24, 2013, \$94,829.82 U.S.-dollar clearing transaction on July 24, 2013, \$14,835.22 U.S.-dollar clearing transaction on August 20, 2013, \$32,663.10 U.S.-dollar clearing transaction on August 28, 2013, and \$118,842.45 U.S.-dollar clearing transaction on April 4, 2014.

780. Additionally, Huawei Co. and Skycom, together with others, knowingly and intentionally conspired to transport, transmit and transfer monetary instruments and funds,

specifically wire transfers, from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, with the intent to IEEPA. the

781. Huawei Co. repeatedly misrepresented to financial institutions that Huawei would not use the financial institution and its affiliates to process any transactions regarding Huawei's Iran-based business. However, Huawei used a U.S. subsidiary of a global financial institution and other financial institutions operating in the United States to process U.S.- dollar clearing transactions involving millions of dollars in furtherance of Huawei's business with Hezbollah, the Qods Force, and Regular IRGC. Some of these transactions passed through this District.

782. As a result of Huawei's scheme and misrepresentations, financial institutions unwittingly cleared hundreds of millions of dollars in transactions that violated U.S. sanctions against doing business with Iran.

783. On information and belief, despite scrutiny from the media, financial institutions, and governmental authorities, Huawei never ceased sourcing U.S.-origin goods and services to Hezbollah, the Qods Force, and Regular IRGC. In addition to sourcing the requested U.S.-origin products and services in contravention of U.S. law, Huawei aggressively pursued relationships with IRGC's, including Hezbollah's and the Qods Force's, fronts, agents, and operatives to protect its lucrative business interests in Iran.

784. While many international vendors withdrew from the Iranian market to avoid violating sanctions, Huawei aggressively secured numerous contracts with both MTN Irancell and MCI to provide telecommunications equipment and services. As reported by the Wall Street Journal on October 27, 2011, Huawei secured numerous contracts with both MCI and MTN

Irancell, and in doing so, agreed to carry out orders from, and support the interests of, Hezbollah, the Qods Force, and Regular IRGC.²⁶⁷

785. The *Wall Street Journal* reported, in relevant part, that Huawei “filled the vacuum” after “Western companies pulled back from Iran after the government’s bloody crackdown on its citizens,” and thereby, Huawei “plays a role in enabling Iran’s state security network.” The *Wall Street Journal* further reported that “a person familiar with Huawei’s Mideast operations” said Huawei’s role included “overseeing parts of the network -- at MTN Irancell, which is majority owned by the government,” and that in 2009 Huawei “carried out government orders on behalf of its client, MTN Irancell, that MTN and other carriers had received to suspend text messaging and block the Internet phone service, Skype, which is popular among dissidents.”

786. Huawei’s agreement to abide by the directives of Hezbollah, the Qods Force, and Regular IRGC was openly promoted by Huawei and the Chinese government. For example, in August 2009, two months after the mass protests began in Iran, the “website of China’s embassy in Tehran reprinted a local article under the headline, ‘Huawei Plans Takeover of Iran’s Telecom Market.’ The article said the company ‘has gained the trust and alliance of major governmental and private entities within a short period,’ and that its clients included ‘military industries.’”²⁶⁸

787. Huawei’s agreement to abide by the directives of the IRGC’s, including Hezbollah’s and the Qods Force’s, fronts, operatives, or agents, was not limited to its work with MTN Irancell. Huawei secured contracts with the largest Iranian mobile network provider MCI,

²⁶⁷ Steve Stecklow, Farnaz Fassihi, and Loretta Chao, *Chinese Tech Giant Aids Iran*, *Wall Street Journal* (October 27, 2011).

²⁶⁸ *Id.*

which is controlled by TCI, by expressly agreeing to provide support for the IRGC's, including Hezbollah's and the Qods Force's, "security" and intelligence objectives.

788. In fact, to secure its place in the Iranian market, Huawei has done "considerable business" with Zaeim Electronic Industries Co. ("ZEI"), an Iranian electronics firm, which is the "**security** and intelligence wing of every telecom bid." ZEI launched its telecommunications division in 2000 in partnership with Huawei and have completed at least forty-six telecommunication projects together. ZEI's website noted its clients include "the intelligence and defense ministries, as well as the country's elite special-forces unit, *the Islamic Revolutionary Guards Corps*."²⁶⁹

789. On information and belief, ZEI was a front for Hezbollah, the Qods Force, and Regular IRGC. ZEI was responsible for "security" functions on more than one IRGC-facing project with respect to more than one western customer, ZEI was closely linked to multiple IRGC addresses and persons, and independent observers concluded the IRGC ran it.²⁷⁰

790. Huawei also assisted the IRGC's, including Hezbollah's and the Qods Force's, fronts, agents, and operatives by installing surveillance equipment, including surveillance equipment used to monitor, identify, and detain protestors during the anti-government demonstrations of 2009 in Tehran, Iran.

791. As reported by the *Wall Street Journal*, and similar to MTN's agreement to assist with "security," Huawei agreed as part of its bid to install MCI's surveillance system to "support and deliver offline and real-time lawful interception," and that, "for public security," the service would allow "tracking a specified phone/subscriber on map."

²⁶⁹ *Id.* (emphasis added)

²⁷⁰ *Id.*

792. Huawei's scheme to provide assistance to the IRGC's, including Hezbollah's and the Qods Force's, fronts, operatives, and agents was not limited to the sourcing of U.S.-origin equipment and technology. For example, Skycom, on behalf of Huawei, employed a U.S. citizen in Iran. Huawei and Skycom were indicted for this unlawful provision of U.S.-based services.

793. Huawei modernized telecommunications technology used by Iranian entities that were controlled by IRGC, including Hezbollah and the Qods Force, fronts, thereby pumping additional revenue into the coffers of Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network.

794. Huawei Co., Huawei USA (after its formation), Huawei Device USA (after its formation), Futurewei, and Skycom provided substantial banned technology to Iranian companies that were controlled by Hezbollah, the Qods Force, and Regular IRGC and, thereby, Huawei's illegally sourced technology ordinarily flowed through to Hezbollah. That banned technology was crucial to perpetrating terrorism. By way of example, terrorists were able to use cell phones and other telecommunication technology and software to perpetrate attacks on Americans.

795. Huawei also assisted the terrorist enterprise by serving as a long-term strategic partner for MTN Irancell and MCI, both of which were fronts for Hezbollah, the Qods Force, and Regular IRGC.

796. Like ZTE, on top of the millions of dollars that Huawei provided to Hezbollah, the Qods Force, and Regular IRGC via TCI (and MCI), Huawei also provided technical aid, including surveillance technology, to Hezbollah, the Qods Force, and Regular IRGC which facilitated terrorism. Huawei Co.'s, Huawei USA's (after its formation), Huawei Device USA's

(after its formation), Futurewei's, and Skycom's technology transfer provided terrorists the ability to intimidate and coerce civilian populations.

797. For a terrorist group intent on targeting Americans traveling in tightly secured convoys or on heavily fortified bases, the technology that Huawei provided bolstered the terrorists' ability to conduct successful surveillance and was vitally important to their ability to execute successful attacks, like the ones that killed and injured Plaintiffs and their loved ones. For these reasons, Huawei's acts, which allowed terrorists access to modern telecommunications technology they could not otherwise obtain, facilitated intimidation, coercion, violent acts, and acts dangerous to human life.

798. The ample evidence of Huawei's own consciousness of guilt supports the inference that Huawei knew it was benefiting the IRGC's, including Hezbollah's and the Qods Force's, terrorist enterprise.

799. As part of the scheme to operate and advance the business of Huawei, including its agreement with the IRGC, to avoid interference in their scheme by U.S. governmental bodies or other private actors, Huawei, Huawei Device USA, and Futurewei repeatedly made material misrepresentations as to their misappropriation and subsequent commercial use of intellectual property, as well as other criminal activity, including the nature and extent of Huawei's business in Iran, to U.S. governmental bodies from whom Huawei, Huawei Device USA, and Futurewei sought regulatory authorization that would help grow Huawei's U.S.-based business.

800. Huawei, Huawei Device USA, and Futurewei made similar material misrepresentations to financial institutions from whom the Defendants sought banking services to process Huawei's and Skycom's Iranian business transactions.

801. Huawei, Huawei USA, Huawei Device USA, and Futurewei made material misrepresentations to the U.S. government about the nature and the scope of Huawei's business activities related to sanctioned countries such as Iran and North Korea, to avoid the economic and regulatory consequences of making truthful statements, including the restriction of Huawei from U.S. markets and business opportunities.

802. In or about 2017, Huawei Co. and Huawei Device USA became aware of the U.S. government's criminal investigation of Huawei and its affiliates. In response to the investigation, Huawei and Huawei Device USA made efforts to move witnesses with knowledge about Huawei's Iran-based business out of the United States and to the People's Republic of China, so that they would be beyond the jurisdiction of the U.S. government, and to destroy and/or conceal evidence located in the United States of Huawei's Iran-based business.

ii. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Substantially Increased MTN Irancell And TCI Revenue By Illicitly Sourcing Embargoed American Technology, Which Flowed Through To The IRGC's Terrorist Proxies

803. From 2008 through at least 2014, Huawei Co.'s, Huawei USA's, Huawei Device USA's, Futurewei's, and Skycom's illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI (including MCI), Exit40, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC which flowed to al-Qaeda and the Taliban and was used to attack Americans in Afghanistan, including Plaintiffs and their loved ones.

804. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom significantly increased the cash flowing through MTN Irancell and TCI, and ultimately being deployed by Hezbollah, the Qods Force, and Regular IRGC. They did so by illicitly supplying

the state-of-the-art American technologies, like servers, to MTN Irancell and TCI, and by extension Hezbollah, the Qods Force, and Regular needed to attack Americans abroad.

iii. Huawei Co., Huawei USA, Huawei Device USA, Futurewei, And Skycom Routed Bribes To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC's Terrorist Proxies

805. Huawei Co. has an extensively documented record of paying bribes around the world in order to win lucrative procurement contracts. Huawei has been credibly accused of procurement-related corruption in, *inter alia*, Namibia,

806. Huawei Co. has pursued an integrated global sales strategy, under which one may infer that Huawei Co. followed the same, or a substantially similar, bribery tradecraft with respect to similar “pitches” for other state-owned telecom companies.

807. Huawei Co.’s “going rate” for bribing decision-makers in the procurement contract setting appears to be approximately one percent (1%) of contract value.

Huawei appears to have paid large sums to a former Serbian state telecom executive through an offshore shell company.

The Chinese tech giant Huawei signed deals to make large payments to two men close to Serbia’s state telecommunications company, using offshore companies that financial crime experts say raise red flags for corruption.

One of these men, former Telekom Srbija executive Igor Jecl, appears to have received over \$1.4 million in contracts, dividends, loans, consulting fees, and an apartment from an offshore company that was paid by Huawei for consultancy. Neither offshore company that dealt with Huawei has a public track record of doing consulting work, or any business at all.

“It is standard with bribery and corruption to dress them up as consultancy,” said Graham Barrow, an expert on financial crime.

Although OCCRP has not uncovered evidence that the payments were improper, they were made over a period of time when Huawei was doing business in Serbia. In 2016, it landed a 150-million-euro deal to upgrade Serbia’s telecommunications infrastructure.

808. On information and belief, from 2008 through 2018, Huawei Co. caused the payment of at least several million dollars, denominated in U.S. Dollars, to one or more officers, agents, or directors of MTN Irancell, TCI, and/or MCI.

iv. Huawei Co, Huawei USA, Huawei Device USA, Futurewei, And Skycom Routed “Free Goods” To The Key Procurement Decisionmakers At MTN Irancell And TCI, Which Flowed Through To The IRGC’s Terrorist Proxies

809. Huawei Co. has a documented history of making a species of “free goods” payment – giving something away at below market pricing to obtain a collateral benefit.

810. On information and belief, Huawei Co. has pursued a similar “free goods” bribery strategy through the sale of below-market-priced communications technologies to its IRGC-affiliated customers.

3. Huawei Knowingly Assumed A Financial, Logistical, And Operational Role In The Taliban’s, Including The Haqqani Network’s, Terrorist Enterprise In Afghanistan, Directly And Indirectly Financing And Arming IRGC Proxy Attacks In Afghanistan And Iraq

811. Huawei operated lucrative businesses in post-invasion Afghanistan by servicing a broad array of customers there. To increase their profit margins by redirecting attacks away from their business interests – and to intentionally assist the Taliban’s effort to drive Americans out of Afghanistan – Huawei knowingly paid protection money to the Taliban, including its Haqqani Network. When Huawei did so, Huawei knowingly assumed a financial, logistical, and operational role in the Taliban’s, including the Haqqani Network’s, terrorist enterprise in Afghanistan and beyond by directly and indirectly routing protection payments to these terrorists in cash and “free goods,” including secure American cell phones.

812. Huawei has become one of the world’s most valuable communications technology manufacturers by providing a comprehensive suite of communications technologies services to customers in high-risk geographies from a counter-terrorism perspective, including geographies

where Hezbollah, the Qods Force, and Regular IRGC and IRGC proxies al-Qaeda and the Taliban, including its Haqqani Network, raised and moved money to facilitate terrorist attacks through protection payments, procurement corruption, “free goods” payoffs, payments routed through consultants, and similar schemes that depended upon complicit corporate partners.

813. Huawei followed that model in Afghanistan, where Huawei has continuously operated for decades.

814. For example, in 2001, “India's intelligence agencies” “placed” “the Chinese telecommunications equipment maker Huawei Technologies Inc.[’s] Indian operations on a watch list for alleged business dealings with the Taliban” after “Indian government” concluded “that Huawei India allegedly helped supply communications surveillance equipment to Taliban forces in Afghanistan.”²⁷¹

815. Huawei’s willingness to directly partner with the Taliban, including its Haqqani Network, continued even after al-Qaeda and the Taliban had launched their nationwide campaign against Americans in Afghanistan after 9/11. Indeed, Huawei was a preferred partner of the Haqqani Network in Pakistan and Afghanistan because Huawei regularly paid the amount requested by the Taliban, including its Haqqani Network. In 2005, for example, the Economic Times (of India) reported how “[a] western multinational telecom company executive was being badgered by a senior bureaucrat to set up a full-fledged mobile network in Jammu and Kashmir,” which were two hotbeds for Syndicate activity in Pakistan:

Given the security environment . . . , and kamikaze not exactly being the guiding philosophy of his [western multinational telecom] company, he had to decline the offer but managed to come up with what he thought was a viable alternative. Since a working relationship with the militants and the Taliban is an essential prerequisite for sustaining operations in the state, why don't you ask Huawei to

²⁷¹ K.C. Krishnadas, *India: Chinese Telecom Firm Supplied Taliban*, Electronic Engineering Times (December 17, 2001), 2001 WLNR 3069135.

take on the task? Well, why not? After all, the [Indian] government has been claiming that Huawei Technologies, the Chinese telecom major, has had links with the Taliban when they ran Afghanistan.²⁷²

816. From 2006 through 2019, Huawei sold products to Afghan telecommunications operators, e.g., MTN Afghanistan, which was MTN's subsidiary in Afghanistan, which were manufactured by the Huawei Defendants.

817. While Huawei was achieving rapid growth in Afghanistan, the communications sector provided a critical source of financing for the Taliban, including its Haqqani Network, in the same manner as it did for Defendant ZTE and co-Conspirator MTN. Huawei's payments mirrored the protection money delivered by ZTE and co-conspirator MTN. Just as the Taliban raised "taxes" from international contractors doing business in Afghanistan, so too did it levy similar "taxes" on "the big telecom companies" like Huawei.²⁷³

818. Huawei's services in Afghanistan required ZTE work in geographies that were controlled or contested by the Taliban, including its Haqqani Network, in which ZTE paid protection payments as a cost of doing business.

819. Huawei's sales to its Afghan customers depended upon ZTE personnel successfully being able to drive large truck convoys containing ZTE's lucrative Afghan-customer-bound goods through Taliban, including Haqqani Network, controlled or contested geographies in Pakistan and Afghanistan.

820. Huawei paid the money as protection: Huawei decided that the cheapest way to shield their projects from attack was to pay the Taliban, including its Haqqani Network to leave them alone and instead attack other targets – like Plaintiffs and their family members. Similar

²⁷² Economic Times (India), *Satyajit Ray Who?* (Sept. 20, 2005), 2005 WLNR 29155896.

²⁷³ Ruttig, *The Other Side* at 20.

payments were pervasive throughout Afghanistan and supplied the Taliban with an important stream of financing to fund their terrorist attacks across the country.

821. The Taliban, including its Haqqani Network, conveyed its protection-money demands to Huawei via Night Letters similar the ones the Taliban sent to ZTE and MTN.

822. Huawei was a particularly aggressive practitioner of protection payments. Rather than invest in expensive security for shipments, Huawei purchased cheaper “security” by buying it from the Taliban, including its post-FTO-designation Haqqani Network.

823. Huawei negotiated its protection payments in direct discussions between Huawei Afghanistan’s security department and Taliban, including Haqqani Network, commanders.

824. Like other contractors in Afghanistan, Huawei generally paid, as protection to the Taliban (including its Haqqani Network), at least ten percent (10%) of its contract budget – and, on information and belief, much more than this – on any contract in which Huawei, including any Huawei affiliate or contractor, provided services to any customer in Afghanistan, since the Taliban controlled or contested every geography in which Huawei worked.

825. Huawei’s practice of making protection payments to the Taliban extended to the Haqqani Network. From at least 2008 through 2017, Huawei operated infrastructure projects sites, and/or sold communications technology products to customers (and therefore transported lucrative commodities through territory) in Afghanistan that was controlled by the Taliban, including its Haqqani Network, and Huawei purchased security for those project sites and shipments by paying the Taliban, including its Haqqani Network. The Haqqani Network’s chief financial operative, Nasiruddin Haqqani, oversaw those payments, and they typically occurred on a semi-annual basis, and the Haqqani Network’s overall involvement in the scheme was

ultimately supervised by Sirajuddin Haqqani, who was at all times a dual-hatted al-Qaeda/Taliban terrorist.

826. Huawei keyed Huawei's rapid growth in Afghanistan by sponsoring a vast stream of payoffs to the Haqqani Network from 2006 through today. Under Sirajuddin Haqqani's leadership, as executed by his immediate family members, the Haqqani Network was responsible for collecting "taxes" from Afghanistan's telecom companies, which were the single largest (legal) industry and tax base in Afghanistan – and thus a key source of funding and power for the Taliban and al-Qaeda, both of which were effectively led by Sirajuddin Haqqani in Afghanistan and Pakistan.

827. The logic behind Huawei's payoffs to the Haqqani Network matched the logic motivating Huawei's joint venture with the IRGC. Huawei's leadership intended to harm American interests in Afghanistan (like Iraq), and supporting the Taliban allowed them to do so. Huawei's decision to route monthly protection payments to al-Qaeda (via Sirajuddin Haqqani and his immediate family members) and the Taliban or face the risk that terrorists commanded by Sirajuddin Haqqani would destroy some of Huawei's shipments. Ordinarily, the going protection payment rate was usually around \$500 to \$2,000 per truck per convoy. In some areas, Huawei caused payments to be made to local Taliban, including Haqqani Network, commanders. In other places, where Huawei operated in a Taliban-controlled environment, the payments would have to be sent to the Taliban's Quetta Shura for southern Afghanistan, e.g., Helmand, or the Taliban's Miram Shah Shura for eastern Afghanistan, e.g., Paktia (Sirajuddin was involved in the former and led the latter).

828. By 2006, the Taliban, including its Haqqani Network, prized the acquisition of western communications technologies, including American-made cell phones, that were “washed” through the IRGC or one of its corporate partners, like Huawei.

829. From 2006 through 2021, Huawei also made protection payments to the Taliban, including its Haqqani Network, in the form of “free goods” – in particular, free communications technologies like cell phones – as an alternative to paying the terrorists in cash. When Huawei did so, Huawei directly provided to the Taliban, including its Haqqani Network, a broad range of communications technologies including, but not limited to, American mobile phones such as American-made Motorola phones, which Huawei reached into the U.S. to specifically acquire for the purpose of transferring such technologies to the IRGC and its proxies, including the Taliban and its Haqqani Network.

830. On information and belief, Huawei transferred millions of U.S. Dollars’ worth of American communications technologies, including more than a thousand (1,000) “free goods” black market American-made cell phones to the Taliban, including its Haqqani Network, which Huawei acquired from the United States and delivered to the Taliban, including its Haqqani Network, each year from 2006 through 2021.

831. Huawei’s transfer of free, and illicitly sourced, communications technologies, including technologies that Huawei sourced from the United States, as a means to bribe the Taliban, including its Haqqani Network, comports with Huawei’s long-standing embrace of “free goods” as a core, decades-long, global strategy to route bribes to recipients.

832. U.S. military and intelligence officials have publicly confirmed Plaintiffs’ allegations against Huawei. For example, on June 8, 2012, *Business Insider* confirmed – citing American “military sources” and “former and current intelligence sources” – that that “China

[was] likely to remain an aggressive and capable collector of sensitive U.S. economic information and technologies.”²⁷⁴ Thus, “[a]nother concern raised by [U.S. military] sources [was] that Huawei and the other Chinese telecommunications companies [i.e., ZTE] also provide[d] technology to Iran and the Taliban.”²⁷⁵ Indeed, “[a]ccording to sources, Iran’s security network relie[d] on Huawei technology.”²⁷⁶

833. When Huawei provided free communications technologies to the Taliban, including black-market American cell phones, Huawei provided the terrorists a cash equivalent that sponsored tremendous violence. At a going rate of \$2,000 per black market cell phone, for example, the value of Huawei’s illicit phones supplied to the Taliban, including its Haqqani Network, delivered at least \$2 million per year in value to the Taliban, including its Haqqani Network.

834. When Huawei acquired and transferred free communications technologies to the Taliban, including black-market American cell phones, from the United States and delivered such technologies to the Taliban, including its Haqqani Network, Huawei provided devastating operational and logistical assistance to the Syndicate in addition to the financial value of such goods through the same operational and logistical benefits that such black-market communications technologies, including American cell phones, accorded to terrorists worldwide.

835. Huawei also directly aided al-Qaeda when Huawei transferred cash and free goods, including the above-described communications technologies and black-market American cell phones, to the Haqqani Network because Sirajuddin Haqqani and his immediate family

²⁷⁴ Business Insider, *Military Sources: China Could Shut Down All The Telecommunications Technology It Sold To America* (June 8, 2012).

²⁷⁵ *Id.*

²⁷⁶ *Id.*

members, who were responsible for collecting protection payments from telecom companies like Huawei, were also members of al-Qaeda, and thus Huawei funded and logistically supplied al-Qaeda when Huawei routed cash and free goods protection payments to the Haqqani family.

836. Huawei's overall payments to the Taliban, including its Haqqani Network, reached millions of dollars in value in cash and "free goods" payments of communications technologies, including black-market American cell phones each year from 2006 through the present. At that rate, the Huawei Defendants caused at least tens of millions in U.S. Dollar-value in cash and "free goods" to flow through to the Taliban, including its Haqqani Network, from 2006 through the present, which furthered the IRGC's conspiracy to attack Americans in Afghanistan and directly aided the IRGC proxies who committed such attacks, i.e., al-Qaeda and the Taliban, including its Haqqani Network, through attacks committed by joint al-Qaeda/Taliban cells and/or attacks committed by the Taliban, including its Haqqani Network, that were planned and authorized by al-Qaeda.

4. Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Including Its Haqqani Network, Comports With Huawei's Historical Sales Practices In International Markets

837. Like MTN and ZTE, Huawei's conduct reflected a willingness to support America's enemies and engage in illicit financial transactions, as a way to increase profits in Iran. The same calculation pervaded Huawei's other conduct throughout the world. Huawei's other conduct further demonstrates its pattern and practice of transacting with violent actors to increase Huawei revenue.

838. Huawei's illicit transactions concerning North Korea demonstrates Huawei's deliberate support for terror.

839. On or about September 13, 2012, a Huawei representative testified before U.S. Congress, testifying that Huawei was not involved in North Korean business interests after 2009. As the Superseding Indictment notes, however, “Huawei was involved in business activities in North Korea, including numerous telecommunications projects, beginning no later than 2008.”

840. Internal Huawei documents obtained by the Department of Justice referred to the geographic location of projects in North Korea with the code “A9”—Huawei’s code for North Korea. Huawei employees concealed Huawei’s involvement in projects in North Korea.

841. For example, shipping instructions provided by Huawei to a supplier in 2013 included the instruction that, for shipments to “A9/NK/NORTH KOREA,” there should be “No HW [HUAWEI] logo,” indicating that Huawei’s corporate logo should not be included on shipments destined for North Korea.

842. Plaintiffs’ allegations concerning Huawei’s willingness to pay bribes and protection payments, in cash and free goods, are also consistent with Huawei’s recent history, as documented by press reports concerning allegations of “rampant corruption” and programmatic bribery by Huawei around the world for decades.²⁷⁷

²⁷⁷ See, e.g., Technode.com, *Another Corruption Scandal Hits Huawei With Its Top Executive Suspected Of Bribery* (Dec. 26, 2017) (“The executive vice president of Huawei’s consumer business group Greater China, Teng Hongfei, has been taken away by the public security... Once a recipient of the highest management honor granted by Huawei, Teng is under investigation for corruption charges... Teng’s fall from grace might have been a result of the rampant corruption inside China’s direct-to-consumer sales, in which retailers often bribe the manufacturers... This isn’t the first time Huawei has found itself in the midst of a corruption scandal. This year started with a bang when six top middle and senior leaders from the consumer business group were accused of giving out internal information... One of the arrested employees was the chief architect of Huawei’s flagship P6 Wu Bin... In 2012, Huawei also found itself in trouble in international waters when Huawei’s Xiao Chunfa was sentenced by an Algerian court along with two other staffers from Chinese smartphone maker ZTE. The trio was tried in absentia for a bribery scandal... They were sentenced to ten years in prison...”), *online at* <https://tinyurl.com/2a9nnsas> (last accessed Apr. 3, 2022); Wall St. J., *Huawei Internal Probe*

5. Huawei's Assistance To Hezbollah, The Qods Force, Regular IRGC, Al-Qaeda, And The Taliban, Including Its Haqqani Network, Had A Substantial Nexus To The United States

843. Huawei's assistance to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied on significant contacts with the United States. Huawei orchestrated both those U.S. contacts and Huawei's violation of U.S. law, including, on information and belief, by and through coordination with Skycom, Huawei Device USA, Huawei USA, and Futurewei. Like MTN and ZTE, Huawei employs a top-down management structure in which Huawei centralizes operational control over the functions performed by its various subsidiaries.

844. Huawei's decision to assist Hezbollah, the Qods Force, and Regular IRGC and by extension their proxies, al-Qaeda and the Taliban, had a substantial nexus to the United States for the reasons explained below.

i. Huawei's Conduct Targeted The United States

845. Huawei's provision of material support to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, was expressly aimed at the United States. At all relevant times, Huawei knew that Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, were targeting the United States. Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, did not conduct an indiscriminate terrorist campaign that merely injured

Finds Possible Evidence of Corruption; Internal Probe Finds 116 Employees May Have Been Involved in Corruption (Sept. 11, 2014) ("Huawei Technologies Co. said [] that a recent internal investigation has found that 116 of its employees may have been involved in corruption... The Chinese telecommunications equipment maker ... didn't provide any further details about the employees in question or the bribery allegations... Chinese media reported last month that Huawei found possible evidence of corruption cases involving 116 employees and hundreds of millions of yuan in bribery.").

Americans by chance. Instead, Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, directed attacks at *Americans* with the specific intent of killing *Americans* in particular – so that they could inflict pain in the United States and influence U.S. policy. Hezbollah’s, the Qods Force’s, Regular IRGC’s, al-Qaeda’s, and the Taliban’s, including its Haqqani Network’s, ultimate, shared, publicly stated goal was to effect a withdrawal of American forces from Afghanistan and the broader Middle East. Each terrorist attack that killed and injured Plaintiffs was part of that campaign of anti-American terrorism.

846. Huawei’s decision to reach into the United States, including by coordinating with Huawei USA, Huawei Device USA, and Futurewei, to obtain embargoed technology to aid the IRGC’s, including Hezbollah’s and the Qods Force’s, terrorist enterprise was also expressly aimed at the United States. Like MTN and ZTE, Huawei knew, based on conversations with IRGC, including Hezbollah and the Qods Force, agents, that Hezbollah, the Qods Force, and Regular IRGC viewed Huawei’s assistance as vital to Iranian national “security,” which Huawei understood to inherently involve the promotion of terrorist violence against Americans around the world as part of Hezbollah’s, the Qods Force’s, and Regular IRGC’s effort to export its Islamic Revolution and drive the U.S. out of Afghanistan.

847. On information and belief, like MTN and ZTE, Huawei also knew, based on conversations with U.S. officials, that it was assuming an active role in an Hezbollah, Qods Force, and Regular IRGC plot to develop cash flow and source vital dual-use components for Hezbollah, the Qods Force, and Regular IRGC proxies, including al-Qaeda and the Taliban. Huawei further knew of the critical importance that communications and computing technology plays for terrorists.

848. When Huawei Co., including by coordinating with Skycom, Huawei USA, Huawei Device USA, and Futurewei, conducted U.S.-based financial transactions denominated in U.S. dollars and sourced embargoed technology that the United States had publicly declared could benefit IRGC, including Hezbollah and the Qods Force, efforts to kill others, they intentionally helped arm terrorists they knew were targeting the United States. On information and belief, Hezbollah, the Qods Force, and Regular IRGC made Huawei agree to a similar contractual pledge as the one in which MTN agreed to aid Iran's "defensive, security, and political" interests outside of Iran. On information and belief, at all times, Huawei knew or recklessly disregarded that "security" was a euphemism for IRGC, including Hezbollah and the Qods Force, terrorist operations outside of the territorial borders of Iran. When Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom executed financial transactions and obtained the technology requested by its IRGC, including Hezbollah and the Qods Force, partners, each took actions in the United States and targeted at United States by helping the terrorists improve their bombs, rockets, communications, and intelligence gathering.

849. Although Huawei's primary motivation for assisting Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban was financial, Huawei also intended to harm Americans in Afghanistan. One reason Huawei cooperated with Hezbollah, the Qods Force, and Regular IRGC was to align itself with their effort to drive Americans out of Afghanistan.

850. Like MTN and ZTE, Huawei intended to harm Americans because it decided that was the necessary price of maintaining a good relationship with Hezbollah, the Qods Force, and Regular IRGC who were explicit, that they expected their partners to provide significant help in fighting against U.S. forces in particular. Thus, for Huawei to achieve its business objectives vis-à-vis Hezbollah, the Qods Force, and Regular IRGC fronts who controlled TCI (including

MCI) and MTN Irancell – both of which Huawei serviced – Huawei needed to disassociate itself from the United States and prove that it could deliver value to the IRGC’s terrorist campaign against U.S. forces in Afghanistan.

851. On information and belief, like MTN, Huawei’s agreement to aid Hezbollah, the Qods Force, and Regular IRGC also fulfilled an obligation by Huawei, like MTN, to engage in “defensive, security and political cooperation” with its IRGC, including Hezbollah and Qods Force, counterparties.²⁷⁸ Such cooperation offered Huawei added motivation for Huawei’s illicit transactions with Hezbollah, the Qods Force, and Regular IRGC counterparties. Huawei’s support for Hezbollah, the Qods Force, and Regular IRGC did not merely grow Huawei’s profits by allowing it to obtain lucrative business from MTN Irancell and TCI (and MCI) in the first instance; it also benefited Huawei’s business by inflicting harm on an enemy (the United States) of one of Huawei’s most important business partners (Hezbollah, the Qods Force, and Regular IRGC) in order for Huawei to curry Iranian favor to gain market share for a potentially uniquely lucrative telecom and communications market (Iran).

852. Plaintiffs’ allegations also comport with the widespread view of relevant U.S. government officials from the executive and legislative branches. For starters, Huawei and its subsidiaries are subject to multiple criminal proceedings for their unlawful conduct with respect to Iran, including the Huawei Criminal Case.

853. Huawei’s scheme to source U.S.-origin technology for Hezbollah, the Qods Force, and Regular IRGC serves and/or conforms to the People’s Republic of China’s broader security and economic interests of competing against the U.S.

²⁷⁸ Exhibit A, MTN-Irancell Consortium Letter Agreement § 8.

854. For example, the Chinese government arrested and jailed several Huawei whistleblowers who claimed that Huawei's business in Iran is an "open secret" and made some of these whistleblowers sign statements pledging to not go against Huawei's public position denying the nature and scope of its Iranian business.

855. Moreover, Huawei previously worked with Panda International Information Technology Co., Ltd. ("Panda Int'l"), a Chinese-state-owned firm, in their joint efforts to help build and maintain North Korea's wireless network using embargoed goods, and to conceal Huawei's sanctions-busting conduct. Thus, Huawei's prior conduct reflects its deference to, and support for, the broader security and economic objectives of the People's Republic of China.

ii. Huawei's Conduct Relied On American Contacts

856. Huawei reached into the United States to acquire U.S.-sourced embargoed technology that it then provided to both MCI and MTN-Irancell.

857. Huawei Co., including but not limited to in coordination with Huawei Device USA, Huawei USA, Futurewei, and Skycom, reached into the United States to support Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, when it obtained technology and vital operational support from the U.S. Huawei supplied technology and operational support for TCI, MCI, and MTN Irancell through various U.S. agents, including but not limited to Huawei Device USA, Huawei USA, and Futurewei. In doing so, Huawei tied its unlawful conduct to the United States by obtaining irreplaceable, best-in-class, and embargoed U.S.-supplied dual-use technology to aid Hezbollah's, the Qods Force's, and Regular IRGC's terrorist enterprise. This U.S. contact was closely related to Huawei's support for Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network.

858. Huawei relied on U.S.-made materials as components for its products for Iran. U.S.-origin goods were technically essential to Huawei's IRGC-related, including its Hezbollah Division-related and Qods Force-related, projects and/or end-users as there were no suitable foreign-made substitutes for many of them.

859. To obtain other U.S.-origin goods for Hezbollah, the Qods Force, and Regular IRGC Huawei Co., along with Huawei USA, Huawei Device USA, and Futurewei misappropriated trade secrets and intellectual property in the United States from American companies and/or companies with American offices.

860. To source U.S.-origin goods and services, including financial services, to the IRGC's, including Hezbollah's and the Qods Force's, fronts, operatives, and agents, Huawei Co., along with Skycom, Huawei USA, Huawei Device USA, and Futurewei conducted financial transactions through the U.S. and with the use of U.S.-based financial institutions or the U.S. subsidiaries of international financial institutions.

861. Huawei, including Huawei USA, Huawei Device USA, and Futurewei agreed to conceal their unlawful conduct in the U.S. related to its support for Huawei's Iranian business interests, including its contracts with both MTN Irancell and MCI. Thus, Huawei, including its American subsidiaries, destroyed documents in the U.S., deleted electronically stored documents, and directed its employees to make false statements to U.S. governmental authorities and financial institutions.

862. The embargoed United States technology included but not limited to servers, switches, routers, and component parts of cellular network infrastructure.

863. Just about every product that Huawei makes has some American components or software in it, such as microchips, modems, and Google's Android operating system.

864. Public reports indicate Huawei helped funnel software and hardware from U.S. firms including Hewlett-Packard, Microsoft Corp, Symantec Corp, and Novell Inc. to the government of Iran between 2008 and 2014.

865. Huawei Co. also unlawfully arranged a U.S. citizen to provide technology services in Iran for Skycom. Simply put, Huawei could not do the business it did with Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, and thereby cause the transfer of key technology to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, without reaching into the United States to obtain the required U.S.-origin goods and services and to conceal and shield its scheme to do so.

866. Huawei Co.'s regular transfers of communications technologies, including American cell phones, to Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, relied upon American contacts, American transactions, American persons, and American service providers, and depended upon Huawei Co. reaching into the United States, or causing agents, cut-outs, or affiliates to reach into the United States, in order to source the premium brand cell phones craved by al-Qaeda and the Taliban at all times after 9/11. On information and belief, from 2005 through present, Huawei Co. regularly reached into the United States to acquire iconic American communication technologies for the Taliban's benefit, including, but not limited to, numerous technological generations, e.g., iPhone 5, iPhone 6, of: (i) Apple's iPhone and iPad, from California, which were among the most popular cell phones in the Middle East after 2008; (ii) Motorola's Two-Way Push-to-Talk Cell Phone, from Illinois, which was widely associated with Hezbollah and its proxies in the Middle East after the broad media coverage of their use during Hezbollah's 2006 attack campaign against Israel; and

(iii) Motorola's Razr Cell Phone, from Illinois, which was one of the most popular cell phones in the Middle East before and after the iPhone.

VII. DEFENDANTS' TRANSACTIONS WITH FRONTS, OPERATIVES, AND AGENTS OF HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, CAUSED FUNDS, ARMS, LOGISTICAL AID, AND OPERATIONAL SUPPORT TO FLOW THROUGH SUCH TRANSACTIONS TO AL-QAEDA AND TALIBAN TERRORISTS AND AIDED AL-QAEDA'S AND THE TALIBAN'S ATTACKS AGAINST AMERICANS IN AFGHANISTAN

A. Hezbollah, The Qods Force, And Regular IRGC Sourced Weapons, Raised Funds, And Obtained Logistical And Operational Support Through Illicit Corporate Transactions In The Telecom, Communications, And IT Sectors

867. As western sanctions clamped down on Iranian terror fronts, Hezbollah, the Qods Force, and Regular IRGC responded by expanding its efforts to obtain funds, purchase weapons and source operational support through illicit corporate transactions in the U.S., U.A.E., and Iran.

868. In so doing, Hezbollah, the Qods Force, and Regular IRGC relied on transactions with multinational corporations, like ZTE Corp. and Huawei Co. (alongside co-conspirator MTN), who operated in key sectors for the dual-use technologies that were essential to the IRGC's, including Hezbollah's and the Qods Force's, communications, surveillance, bombmaking, rocket attacks, intelligence gathering, and project management – everything a transnational terrorist group needs to coordinate attacks against Americans in the Middle East.

869. Sadegh Zibakalam, a professor of political science at the University of Tehran, explained to the BBC in 2012 that “[d]uring the past decade Iran has come up with various ways of getting around international sanctions.”²⁷⁹ Per the BBC, Professor Zibakalam “said Iranian companies had been able to source many American ... goods through international markets,

²⁷⁹ BBC News, *Iran Mobile Operator Irancell ‘Secures US Technology’* (June 6, 2012).

especially companies based in Dubai ... He added that international companies have been eager to assist Iran with equipment it needs.”²⁸⁰

870. Hezbollah, the Qods Force, and Regular IRGC relied upon the use of concealment and corporate covers to illicitly acquire the technology necessary to continue to scale its conspiracy. At all relevant times, Hezbollah, the Qods Force, and Regular IRGC operated purpose-built units designed to extract American technology for use by Hezbollah and the Qods Force by coordinating with organized crime and facilitators. Indeed, the IRGC’s use of crooked corporations as fronts is consistent with longstanding IRGC terrorist doctrine, which emphasizes the use of mafia-like “buffers,” cut-outs, and fraud schemes designed to route value and services without leaving a paper trail: in short, IRGC terrorist tradecraft.

871. It is widely understood globally that illicit transactions that route money or technology to the IRGC inevitably result in its Hezbollah Division and the Qods Force receiving money, technology, or services that it can use in its terrorist enterprise, and vice versa.

872. Scholars who have studied Hezbollah, the Qods Force, and Regular IRGC concur that both benefit from illicit transactions and that the purported distinction between them is largely immaterial when it comes to Iran’s terrorist enterprise and support for terrorist proxies. For example, British researcher Ben Smith, who studied Hezbollah, the Qods Force, and Regular IRGC for the House of Commons, identified telecoms as a key area that financially benefits all:

[T]he Revolutionary Guards, have ***large and expanding business interests*** ... The Iranian economy is “marked by a bloated, inefficient state sector”. That has allowed the president to appoint allies and old colleagues from the Revolutionary Guard into key positions in the public sector, and to award government contracts to companies owned ***or*** controlled by Guard members, many of which are involved in dual use technology ... ***including telecommunications*** ... The ***al-Quds force is thought to be no less involved in the business world than the rest of the Revolutionary Guard***, and analysts suspect that these growing business

²⁸⁰ *Id.*

interests provide *clandestine sources of funding to be channelled to overseas groups and individuals, hidden from [] scrutiny* ...²⁸¹

873. Prominent media reports also support this conclusion. According to a 2007 report in *The New York Times*, “[s]ome specialists even question whether the Quds Force exists as a formal unit clearly delineated from the rest of the Revolutionary Guard.”²⁸² As one such Iran specialist, Vali R. Nasr of the Naval Postgraduate School explained to the *Times*, “[i]t could be that anyone with an intelligence role in the Revolutionary Guard is just called Quds.”²⁸³

874. Moreover, any lines between the IRGC and the Qods Force blur when it comes to Iran’s support for Islamist terrorists outside of Iran. As the same *New York Times* report noted in 2007, “[w]hether properly identified as part of the Quds Force or not, members of the Revolutionary Guard mobilized intelligence and paramilitary agents in Lebanon in the 1980s, where they trained the Shiite militia Hezbollah; in Afghanistan, during the anti-Soviet jihad in the 1980s and episodically since then; in the former Yugoslavia, supporting the Bosnian Muslims against Serbian forces; and in other trouble spots.”²⁸⁴

875. As the Foundation for Defense of Democracies similarly concluded, given the tight nexus between IRGC commercial activity and violence by Iranian proxies, any transaction with IRGC fronts benefits Iran’s terrorist enterprise – even when it does not result in the IRGC or Qods Force directly obtaining any embargoed arms or technology:

IRGC front companies ... have stakes in telecommunications of which Iran is the largest manufacturer in the Middle East. ... Many IRGC projects are military in nature, and the group *diverts much of the technology and expertise it*

²⁸¹ Ben Smith (International Affairs and Defence Section of the UK House of Commons Library), *The Quds Force of the Iranian Revolutionary Guard -- Standard Note: SN/IA/4494*, UK House of Commons Library Standard Note (Oct. 30, 2007) (emphasis added).

²⁸² Scott Shane, *Iranian Force, Focus of U.S., Still a Mystery*, N.Y. Times (Feb. 17, 2007).

²⁸³ *Id.*

²⁸⁴ *Id.*

acquires from Western companies for seemingly innocuous projects to unsavory ends. ... Any company that does business in Iran risks becoming an unwitting accomplice to the IRGC's nefarious activities ... Yet even when companies provide services and technologies that cannot be diverted to illicit projects, partnering with the IRGC entails some complicity with its activities. In June 2006, [the head of an IRGC-owned company] confirmed in an interview with a local daily that the *organization's funds finance various national defense projects, including arming and training Hezbollah.*²⁸⁵

B. Defendants Made Illicit Deals With Hezbollah, Qods Force, And Regular IRGC Fronts, Operatives, Agents, And Cut-Outs That Caused Secure American Smartphones, Enterprise Level Servers, Network Computing Technologies, And Weapons To Flow Through The IRGC To Al-Qaeda And The Taliban And Facilitate Terrorist Attacks On Americans in Afghanistan

876. Beginning in 2005, after Hezbollah, the Qods Force, and Regular IRGC had intensified its support of the terrorist campaign in Iraq, ZTE Corp. and Huawei Co. (alongside their co-conspirator MTN) made illicit deals with IRGC, including Hezbollah and the Qods Force, fronts, operatives, agents, cut-outs, and Orbits in the telecom, communications, and network computing sectors. Those deals directly benefited ZTE Corp. and Huawei Co. (alongside co-conspirator MTN), and caused tens of millions of dollars' worth of embargoed American technologies to flow into the IRGC's (including Hezbollah's and the Qods Force's) terrorist enterprise each year.

877. Hezbollah, the Qods Force, and Regular IRGC was able to leverage Defendants' insatiable appetite for Iran's telecom market, which was widely understood to represent a unique opportunity. As *The Economist* explained in 2004, "[w]ith a population of some [70 million people] and a mobile-phone penetration rate of below 5%, *Iran offers a unique opportunity for*

²⁸⁵ Mark Dubowitz and Emanuele Ottolenghi (Foundation for Defense of Democracies), *The Dangers Of Doing Business With Iran's Revolutionary Guards*, *Forbes* (June 15, 2010) (emphasis added).

telecommunications investors. ... However, the wrangles with ... Turkcell illustrate the difficulties in assessing the political risk associated with trying to enter the Iranian market.”²⁸⁶

878. ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) engaged in virtually identical conduct throughout the course of the conspiracy. Since MTN Group joined the conspiracy in 2005, ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) have each acted in a manner consistent with terrorist operations, and each of them have demonstrated the ability to execute complex financial frauds spanning multiple continents without detection, bearing all the hallmarks of the IRGC’s terrorist tradecraft.

879. ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) followed a common tradecraft when pursuing their illicit acquisitions of embargoed American technologies for Hezbollah, the Qods Force, and Regular IRGC.

880. ZTE Corp.’s and Huawei Co.’s (alongside co-conspirator MTN’s) transactions provided financial, technical, logistical, and operational support to Hezbollah, the Qods Force, and Regular IRGC worth tens of millions of U.S. dollars per Defendant each year, which funds their terrorist proxies including, but not limited to, Jaysh al-Mahdi in Iraq, al-Qaeda (worldwide), and the Taliban, including its Haqqani Network, in Afghanistan.

881. ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) furthered the conspiracy by ensuring its concealment for years through their rigorous adherence to the core principles of terrorist tradecraft specifically practiced by the IRGC, including its Hezbollah Divisions and Qods Force, while performing “security”-related operations, e.g., Qods Force facilitation of al-Qaeda/Taliban attacks in Afghanistan. Defendants’ rigorous adherence to IRGC

²⁸⁶ Economist Intelligence Unit, *Iran: Putting Up The Shutters*, Business Middle East (Sept. 1, 2004) (emphasis added), 2004 WLNR 10893473.

terrorist tradecraft furthered the conspiracy because it provided concealment to the fronts, operatives, and illicit transactions that channeled millions through to Hezbollah, the Qods Force, and Regular IRGC and through them, to the IRGC's terrorist proxies worldwide.

882. ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) deployed numerous illicit strategies to covertly route embargoed American smartphones, servers, network computing systems, and the associated technical support services without which their high-end gear was of little value. While the strategies differed over time, each shared a common specific intent: to cause tens of millions in valuable state-of-the-art American technologies, services, and currency to flow from the United States to Hezbollah, the Qods Force, and Regular IRGC and through them, to the IRGC's Shiite and Sunni terrorist proxies worldwide, in order to sustain the terrorist campaigns in Iraq, Afghanistan, Yemen, Syria, and Europe.

883. While Defendants pursued several different strategies for flowing terrorist finance through the MTN Irancell and TCI fronts to the IRGC terrorists standing behind it, two had the greatest impact.

884. Defendants' illicit deals with Hezbollah, the Qods Force, and Regular IRGC fell into three broad categories of deal type: (1) weapons procurement through sham deals; (2) financing through illicit transactions; and (3) operational support obtained through the legitimacy of the companies helping Hezbollah, the Qods Force, and Regular IRGC.

885. Although Defendants' illicit transactions with, and resulting cash flow to, fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC provided especially valuable assistance for al-Qaeda's and the Taliban's terrorist attacks, the causal nexus was not limited to Iran sanctions violations. Whether or not ZTE and Huawei (alongside co-conspirator MTN) technically violated Iranian sanctions (although they did), their transactions with a

counterparty that was openly controlled by terrorists – and which openly diverted the fruits of the transactions to terrorist ends – supplied Hezbollah, the Qods Force, and Regular IRGC Hezbollah, and through them, al-Qaeda and the Taliban, with funds, weapons, weapons components, computers, communications gear, enterprise data management solutions, and essential logistical support upon which the Syndicate relied to commit terrorist attacks against Americans in Afghanistan.

886. Defendants knowingly helped Hezbollah, the Qods Force, and Regular IRGC source hundreds of distinct items of state-of-the-art embargoed American technology that was illicitly acquired within the U.S. and then re-exported to Defendants’ respective IRGC-front counterparties, to be given to terrorists. Plaintiffs offer representative examples of the “security” assistance that Defendants provided MTN Irancell and TCI (including MCI).

887. For decades, Hezbollah, the Qods Force, and Regular IRGC have recognized the centrality of cell phones to the modern terrorist. Hezbollah has long widely deployed mobile phones as a tool of terror.

888. ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) deliberately engaged in complex schemes to acquire sensitive American technologies on the black market, and route the “security” assistance to Hezbollah, the Qods Force, and Regular IRGC.

C. Defendants Made Illicit Deals With Hezbollah, Qods Force, And Regular IRGC Fronts, Operatives, Agents, And Cut-Outs That Caused Substantial Funds To Flow Through The IRGC To Al-Qaeda And The Taliban And Facilitated Terrorist Attacks Against Americans In Afghanistan

889. Beginning in 2005, after Hezbollah, the Qods Force, and Regular IRGC had intensified its support of the terrorist campaign in Afghanistan, ZTE Corp. and Huawei Co. (alongside co-conspirator MTN) made illicit deals with IRGC, including Hezbollah and the Qods Force, fronts, operatives, agents, cut-outs, and Orbits in the telecom, communications, and

network computing sectors. Those deals directly benefited ZTE Corp. and Huawei Co. (alongside co-conspirator MTN), and caused tens of millions of U.S. dollars to flow into the IRGC's (including Hezbollah's and the Qods Force's) terrorist enterprise each year.

1. Procurement Bribery

890. At all relevant times, the IRGC operated one of the most corrupt procurement environments in the world.

891. The IRGC's approach was not out of line with prevailing Iranian corruption practices. As one trade publication explained, "[c]orruption" is [a] [k]ey [c]oncern," in Iran "[a]nd [w]ill [l]ikely [w]orsen" because "[a]n endemic culture of corruption appears to pervade all areas of society in Iran, presenting a major obstacle for private and foreign-owned businesses."²⁸⁷ Indeed, "Iran provides a highly conducive environment for corruption to flourish, primarily due to the opaque and complex nature of government, and the convoluted process of completing bureaucratic procedures."²⁸⁸

892. Under official IRGC, including Hezbollah and the Qods Force, policy, Hezbollah, the Qods Force, and Regular IRGC follows a mafia-style financial approach under which all IRGC, including Hezbollah and Qods Force, fronts, operatives, agents, cut-outs, and Orbits share a percentage of all income they realize with Hezbollah, the Qods Force, and Regular IRGC like how a mafia lieutenant kicks up a portion of his earnings to the mob boss. For example, in 2003, the IRGC issued a directive decreeing that profits realized by IRGC fronts, operatives, and agents must be shared with the broader IRGC organization, i.e., its Hezbollah Division and Qods Force. The IRGC issued this directive as it was ramping up for a long multi-front terrorist

²⁸⁷ Emerging Monitor Online, *Iran: Major Barriers To Investment* (Feb. 19, 2016), 2016 WLNR 5299681.

²⁸⁸ *Id.*

campaign against the United States, and the point of the directive was to escalate the flow of funding supporting the IRGC's terrorist proxies in Iraq and Afghanistan.

893. Hezbollah, the Qods Force, and Regular IRGC have long emphasized weaponizing their control (directly or indirectly) of procurement processes to generate cash flow.

894. Acting through its Hezbollah Division, the IRGC has long counseled its terrorist proxies about the utility of seizing government ministries, state-owned-enterprises, and private commercial businesses in order to convert them into tools of terrorist finance.

895. IRGC Shiite Terrorist Proxies made this a calling card of IRGC-backed terror, having deployed the strategy in every IRGC-backed terror campaign since the Islamic Revolution in 1979, including Hezbollah's control of social services in Lebanon, Jaysh al-Mahdi's control of the Iraqi Ministry of Health, and the Houthis' control of certain geographies in Yemen, as three examples.

896. From the perspective of an operative, agent, cut-out, cover, or proxy ally of Hezbollah, the Qods Force, and Regular IRGC the IRGC's procurement bribery tradecraft usually calls for the following principles:

- (i) for ordinary procurement projects, e.g., a captive ministry purchasing a supply of commodities, the terrorist should extract a bribe or kickback of ten percent or more (and regularly much more), often styled as a *khums* and delivered in cash (U.S. Dollars required) or "free goods";
- (ii) for mega-blockbuster procurement projects, e.g., build the complete nationwide infrastructure for a communications device, the terrorist should extract whatever the terrorist can get, but should not get greedy or let the perfect be the enemy of the good (the terrorist analogue to the maxim "pigs get fat, hogs get slaughtered"); and
- (iii) regardless of project type, follow similar terrorist tradecraft, including, but not limited to, emphasis on concealment and covers.

2. “Free Goods”

897. Hezbollah, the Qods Force, and Regular IRGC have long emphasized manipulation of local and regional black markets as an ideal source of cash flow.

898. The IRGC has long preferred “free goods” bribes as a tool of terrorist finance because “free goods” serve as cash equivalents given the ease of black-market access throughout the region, and “free goods” do not leave as large (or any) of a paper trail.

899. Hezbollah, the Qods Force, and Regular IRGC and every IRGC Shiite Terrorist Proxy, has deep experience monetizing every conceivable type of “free good” on the black market because every such terrorist group draws most of its members from geographies where black markets have been endemic for decades, including several where certain goods could only be acquired on the black market (e.g., medicine in Syria during the violence).

900. Hezbollah, the Qods Force, and Regular IRGC specifically trained its operatives with respect to terrorist tradecraft concerning cell phones, including, but not limited to, how a terrorist can treat cell phones as cash equivalents to be sold or traded like any other precious commodity, e.g., gold, in support of the conspiracy.

901. Hezbollah, the Qods Force, and Regular IRGC also taught its operatives that they could use their mobile phones as cash equivalents.

902. This is important because each Defendant caused thousands, if not tens of thousands, of secure American mobile phones, to flow through MTN Irancell and/or TCI to the terrorists.

903. The going rate for a “clean” American cell phone on the black market is a 10X markup. The phones that get busted out into this market are ordinarily priced at around \$200 per phone (because the annual contract heavily subsidizes the device itself). Thus, when black

market sellers flip an ordinary American cell phone, they can expect to earn about \$2,000 per black market cell phone.

904. The IRGC's historic preference for "free goods" as a form of terrorist finance was met by Defendants' willingness to spend their own money to buy American mobile phones for Hezbollah, the Qods Force, and Regular IRGC. Each Defendant understood that it could curry favor with its IRGC business partner by flooding the zone with untraceable American smartphones.

905. On information and belief, Defendants supplied free mobile phones to Hezbollah, the Qods Force, and Regular IRGC because Defendants understood that Hezbollah, the Qods Force, and Regular IRGC as well as Shiite terrorist proxies like Jaysh al-Mahdi, have long emphasized the exploitation of black markets to derive untraceable terrorist cash flow. Such a view comports with the IRGC's intense doctrinal focus on concealment as the first virtue of a "security" operatives, and the paranoia that IRGC personnel could be detected by the "Great Satan." Black markets are safely anonymous.

906. Moreover, for decades, corrupt companies in the Middle East have leveraged "free goods" schemes to route bribes to Iran-backed terrorists, and as a result, at all relevant times there has been a thriving "corruption economy" that roughly traces the "Shiite Crescent" from Iran through Iraq into Syria and terminating in Lebanon. Given the pervasive black markets that flourishes here, and throughout the Middle East, Asia, and Africa, so-called "free goods" bribery schemes offer several ideal features for the hardened corporate criminal (or terrorist), including built-in cover if detected (e.g., "we are just a civilian phone company").

907. Indeed, free goods are an especially potent form of terrorist finance for Hezbollah, the Qods Force, and Regular IRGC because free goods (in the form of technologies like mobile

phones) are usually compact, lucrative, odorless, valuable, and easy to unload on the black market. Moreover, free goods offer an enormous tradecraft benefit for terrorists – no paper trail and no electronic or data signature for the Americans to capture.

908. Defendants’ “free goods” to Hezbollah, the Qods Force, and Regular IRGC flowed through to benefit al-Qaeda and the Taliban, including its Haqqani Network, in furtherance of the IRGC’s Conspiracy. Defendants’ provision of free phones to the IRGC caused more frequent, effective, and lethal al-Qaeda and Taliban IED attacks against Americans in Afghanistan by furnishing Hezbollah and the Qods Force with IED bombmaking materials to supply to al-Qaeda and the Taliban, which helped the Syndicate source bomb components and also improved the effectiveness of such Afghan terrorists’ IED attacks against Americans by defeating the U.S. counter-IED technologies with which the IRGC was familiar from Iraq.

3. Exit40

i. Exit40 Was An IRGC Front

909. Hezbollah, the Qods Force, and Regular IRGC have active cells in India, Switzerland, and the U.A.E., and rely upon all three as critical geographies to flow through precious U.S. Dollars and illicitly acquired American technologies, ultimately flowing back to the IRGC’s Hezbollah Division and Qods Force, to be used to aid the attack campaigns in Iraq, Afghanistan, and elsewhere in furtherance of the IRGC’s Conspiracy.

910. Exit40 was a company with letter box offices in the U.A.E., Florida, India, and Switzerland. On information and belief, Exit40 was a front company created by or for Hezbollah and the Qods Force, and owned, controlled, and operated by Hezbollah.

911. On information and belief, Exit40 was purpose-built by Hezbollah and the Qods Force, following IRGC terrorist tradecraft, to serve as a Hezbollah front for illicit fundraising and acquisition of embargoed U.S. technologies including American smartphones and servers.

912. On information and belief, Exit40 supplied the described Security Aid to Hezbollah, the Qods Force, and other IRGC-affiliated terrorists and/or proxies in order to, among other things, aid attacks by the IRGC Syndicate Terrorist Proxies in Afghanistan.

913. On information and belief, Hezbollah and the Qods Force used Exit40 to extract millions of U.S. Dollars and tens of millions worth of American technologies, from inside the United States, through a hub location overseas (e.g., Singapore) before reaching the relevant terrorist cell in Afghanistan, Iraq, Iran, Pakistan, or the U.A.E.

ii. Co-Conspirator MTN Group Knowingly Used Exit40 To Finance Hezbollah And The Qods Force

914. MTN Group and MTN Dubai had a business relationship with Exit40.

915. MTN Group and MTN Dubai have gone to extreme lengths to conceal their business relationship with Exit40. Among other things, MTN Group and MTN Dubai employees have been instructed not to mention Exit40 over the phone or in an email.

916. On information and belief, MTN Group and MTN Dubai personnel discouraged any telephonic or email discussions concerning Exit40 because they knew the relationship with Exit40 to be illegal, they believed Exit40 was acting on behalf, directly or indirectly, of Hezbollah, the Qods Force, and Regular IRGC to facilitate attacks against Americans.

917. On information and belief, an operative, employee, agent, or cut-out from MTN Irancell, TCI, the Bonyad Mostazafan, or another IRGC-controlled entity, made MTN Group and MTN Dubai aware that MTN Group and MTN Dubai should use Exit40 in order to help source the U.S. Dollars and American technologies that Hezbollah, the Qods Force, and Regular IRGC needed to deploy in furtherance of the IRGC's terrorist conspiracy and attack campaign against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

918. On information and belief, MTN Group caused the retention of Exit40 by MTN Group, MTN Dubai, or MTN Mauritius, so that Exit40 would serve as MTN Group's, MTN Dubai's, MTN Irancell's and/or TCI's agent or cut-out in order to intentionally route U.S. Dollars and embargoed American technologies through the MTN-related entities, so that some or all of the associated funds or technologies flowed through to Hezbollah, the Qods Force, and Regular IRGC to be deployed in furtherance of the IRGC's terrorist conspiracy and attack campaign against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

919. MTN Group caused MTN Group personnel, MTN Dubai, or an MTN subsidiary, affiliate, agents, cut-out, or business partner to pay millions of U.S. Dollars to Exit40 in order to cause Exit40 to procure the embargoed American technologies identified by Hezbollah, the Qods Force, and Regular IRGC in order to support the IRGC's terrorist conspiracy and attacks against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

920. On information and belief, such transactions by MTN Group and MTN Dubai, or caused by MTN Group and MTN Dubai, routed millions of U.S. Dollars and American technologies from the United States to the terrorists overseas from on or about 2005 through on or about 2012, which discovery should reveal.

iii. ZTE Corp. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force

921. On information and belief, ZTE Corp. had a business relationship with Exit40. Plaintiffs' belief is based upon, among other things, the nature of the conspiracy, requirements of IRGC tradecraft, and specific indicia unique to Exit40.

922. ZTE Corp. destroyed vast amounts of data. On information and belief, the data ZTE Corp. destroyed included data relating to Exit40.

923. On information and belief, an operative, employee, agent, or cut-out from MTN Irancell, TCI, the Bonyad Mostazafan, or another IRGC-controlled entity, made ZTE Corp. aware that ZTE Corp., or an affiliate, subsidiary, cut-out, or agent of ZTE Corp., should use Exit40 in order to help source the U.S. Dollars and American technologies that Hezbollah, the Qods Force, and Regular IRGC needed to deploy in furtherance of the IRGC's terrorist conspiracy and attack campaign against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

924. On information and belief, ZTE Corp. caused the retention of Exit40 by either ZTE Corp. or another ZTE subsidiary, affiliate, or agents, so that Exit40 would serve as ZTE Corp.'s, MTN Irancell's and/or TCI's agent or cut-out in order to intentionally route U.S. Dollars and embargoed American technologies through the ZTE-related entities, so that some or all of the associated funds or technologies flowed through to Hezbollah, the Qods Force, and Regular IRGC to be deployed in furtherance of the IRGC's terrorist conspiracy and attacks against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

925. On information and belief, ZTE Corp. caused ZTE Corp. personnel, or a ZTE subsidiary, affiliate, agents, cut-out, or business partner to pay millions of U.S. Dollars to Exit40 in order to cause Exit40 to procure the embargoed American technologies identified by Hezbollah, the Qods Force, and Regular IRGC in order to support the IRGC's terrorist conspiracy and attack campaign against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

926. On information and belief, such transactions by ZTE Corp., or caused by ZTE Corp., routed millions of U.S. Dollars and American technologies from the U.S. to the terrorists overseas from on or about 2005 through on or about 2012, which Discovery should reveal.

iv. Huawei Co. Knowingly Used Exit40 To Finance Hezbollah And The Qods Force

927. On information and belief, Huawei Co. had a business relationship with Exit40. Plaintiffs' belief is based upon, among other things, the nature of the conspiracy, requirements of IRGC tradecraft, and specific indicia unique to Exit40.

928. Huawei Co. destroyed vast amounts of data. On information and belief, the data Huawei Co. destroyed included data relating to Exit40.

929. On information and belief, an operative, employee, agent, or cut-out from MTN Irancell, TCI, the Bonyad Mostazafan, or another IRGC-controlled entity, made Huawei Co. aware that Huawei Co., or an affiliate, subsidiary, cut-out, or agent of Huawei Co., should use Exit40 in order to help source the U.S. Dollars and American technologies that Hezbollah, the Qods Force, and Regular IRGC needed to deploy in furtherance of the IRGC's terrorist conspiracy and attacks against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

930. On information and belief, Huawei Co. caused the retention of Exit40 by either Huawei Co. or another Huawei subsidiary, affiliate, or agents, so that Exit40 would serve as Huawei Co.'s, MTN Irancell's and/or TCI's agent or cut-out in order to intentionally route U.S. Dollars and embargoed American technologies through the Huawei-related entities, so that some or all of the associated funds or technologies flowed through to Hezbollah, the Qods Force, and Regular IRGC to be deployed in furtherance of the IRGC's terrorist conspiracy and attack campaign against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

931. On information and belief, Huawei Co. caused Huawei Co. personnel, or a Huawei subsidiary, affiliate, agents, cut-out, or business partner to pay millions of U.S. Dollars to Exit40 in order to cause Exit40 to procure the embargoed American technologies identified by Hezbollah, the Qods Force, and Regular IRGC in order to support the IRGC's terrorist conspiracy and attack campaign against Americans in Afghanistan, Iraq, Yemen, and elsewhere.

932. On information and belief, such transactions by Huawei Co., or caused by Huawei Co., routed millions of U.S. Dollars and American technologies from the U.S. to the terrorists overseas from on or about 2005 through on or about 2012, which Discovery should reveal.

D. Defendants’ Protection Payments To The Taliban, Including Its Haqqani Network, Directly Aided Terrorist Attacks On Americans In Afghanistan

933. Defendants’ conduct aided the Taliban’s terrorist enterprise. The very nature of the protection-money demands – backed by violent threats conveyed by the same Taliban fighters who were waging an insurgency against the United States – ensured a close connection between the payments and subsequent Taliban attacks on American forces. Such attacks were a necessary consequence of Defendants’ payments. When they paid the Taliban protection money, they were not lessening the overall risk of terrorist violence; they were paying the Taliban to redirect its attacks to other targets. One prevailing slogan among private-security contractors in Afghanistan captured that mentality: contractors often said “you want them to fight Big Army [*i.e.*, the U.S. Army] before they fight you.” Defendants’ payments accomplished exactly that. They paid the Taliban to attack Coalition forces rather than Defendants’ own businesses.

934. Defendants’ protection payments supplied the Taliban with an important stream of revenue it used to finance terrorist attacks against Americans in Afghanistan. Defendants’ protection payments, which created an income stream overseen directly by Quetta leadership, gave the Taliban fungible resources that were vital to its ability to sustain its terrorist enterprise. For that reason, the Commission on Wartime Contracting observed that “diverted funds,” channeled from Western contractors to the Taliban, “directly strengthen the insurgency.”²⁸⁹

²⁸⁹ *CWC Report* at 74.

935. The Taliban institutionalized control of its protection-money revenue. The extraction of protection payments occurred via a highly regulated process designed to ensure that such payments would benefit the broader insurgency. The Taliban’s 2009 Code of Conduct, for example, contained extensive regulations dictating to local field commanders how to collect (and spend) protection money from foreign businesses. As Ms. Peters explained, those regulations “literally institutionaliz[ed] how profits earned from organized crime are to be distributed within the command chain.”²⁹⁰ The money flowed both ways – from local commanders up to the Financial Commission for use by the Taliban’s central leadership, and conversely from the leadership back down to local commanders for use in the field. In all cases, the Quetta Shura maintained “final say in all matters of collecting protection money.”²⁹¹ That discipline allowed protection money collected from all over the country to finance the Taliban’s terrorist machine.

936. Defendants’ protection payments similarly financed the Haqqani Network. Not only did Defendants fund the Haqqanis directly, but their payments to the Taliban likewise financed Haqqani operations. The Haqqani Network was part of the Taliban and operationally intertwined with Taliban leadership. For that reason, according to a declassified 2009 DIA cable, “a large majority of the Haqqani Network (HQN) funding comes from the Quetta . . . , Pakistan-based Taliban leadership.”²⁹² As Ms. Peters concluded, the Haqqani Network relied on the Taliban organization to “cover operational costs,” with the amount of financing depending on “the funding capacity of the Taliban leadership.”²⁹³ The money flow went both ways: payments

²⁹⁰ *Crime & Insurgency* at 16.

²⁹¹ *Id.* at 17.

²⁹² Def. Intelligence Agency, *Afghanistan – Haqqani Network Finances* (Sept. 24, 2009).

²⁹³ Gretchen Peters, *Haqqani Network Financing: The Evolution Of An Industry* at 23, Combatting Terrorism Ctr. (July 2012) (“*Haqqani Network Financing*”).

to the Taliban supported Haqqani attacks, and payments to the Haqqani Network supported Taliban attacks.²⁹⁴

1. Defendants' Cash Protection Payments To The Taliban, Including Its Haqqani Network, Directly Funded Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan

937. Money supplied the lifeblood of the Taliban insurgency. Financing gave the Taliban the means to recruit and pay terrorist fighters; to acquire weapons and explosives with which to attack Coalition forces; and to maintain the vast operational infrastructure needed to sustain the insurgency. In 2011, it cost the Taliban an estimated \$100-155 million overall to launch attacks and up to \$300 million to “maintain[] the insurgency” generally.²⁹⁵ Those costs ballooned as the insurgency intensified. As a U.N. Security Council report documented, from 2006-2012, the Taliban “managed to finance an ever-increasing number of attacks, reflecting a year-on-year increase in income.”²⁹⁶ The Taliban’s access to financing was vital to its ability to sustain its growing campaign of terrorism against the United States. As one military historian observed in 2011, “the Taliban’s most significant weapon is not its arms or its ability to mobilize jihadists but the vast sums of money that it seems to have at its disposal.”²⁹⁷

938. Protection payments supplied the Taliban with the means to buy weapons and explosives for use in terrorist attacks. Weapons capable of killing and injuring Americans cost money, and Defendants’ protection payments provided the Taliban with a potent source of funding to cover the cost of its escalating insurgency. As Ms. Peters explained, once companies

²⁹⁴ *Crime & Insurgency* at 33 (Quetta Shura agreed with the Haqqani Network “to operate alongside each other and to divide the proceeds they earn in some zones where more than one faction operates.”).

²⁹⁵ *U.N. Financing Report* ¶ 34.

²⁹⁶ *Id.*

²⁹⁷ *Follow The Money*.

decided to “pay off insurgents to avoid having [their] projects attacked,” the “insurgents then spen[t] the money they raise[d] to purchase weapons and explosives, which in turn get used to kill American soldiers.”²⁹⁸ Congressman Bill Delahunt was even more succinct. Responding to reports that “U.S.-funded contractors” made “protection payments to the Taliban,” he observed: “That translates into money that the Taliban are using to attack and kill American military personnel, and that’s just simply outrageous.”²⁹⁹

939. Even relatively small protection payments had an outsized effect on the Taliban’s terrorist capabilities. Although estimates vary, the Taliban paid many of its rank-and-file fighters about \$100 per month, while mid-level commanders made upwards of \$350 per month. As for many of the IEDs that the Taliban used against Coalition troops, a Pakistani security official estimated that they cost a mere \$100 to make.³⁰⁰ At those rates, even a single protection payment of \$2,000 could finance substantial insurgent violence: it could put ten fighters and a commander in the field for a month, and supply them with five IEDs. And Defendants each made payments that were many orders of magnitude higher. Those payments materially strengthened the Taliban’s ability to finance the attacks that killed and injured Plaintiffs.

940. The effect of protection payments was especially pronounced because they enabled Taliban commanders to pay recruits who fought against the Coalition for financial (rather than ideological) reasons. Taliban commanders typically operated on thin margins and faced constant pressure to raise enough money both to pay fighters and to launch attacks. Protection money was essential to fulfilling both needs: had Defendants refused to pay and cut

²⁹⁸ *Id.* at 31.

²⁹⁹ Nancy Cordes, *Is Taxpayer Money Funding The Taliban?*, CBS News (Sept. 3, 2009).

³⁰⁰ See Kathy Gannon, *Taliban Gains Money, al-Qaida Finances Recovering*, Assoc. Press (June 20, 2009).

off that source of revenue, it would have forced Taliban commanders to “deci[de] between paying and feeding [their] troops and launching attacks.”³⁰¹ Defendants’ payments freed Taliban commanders from that choice and enabled them to retain their fighters while continuing with attacks on Coalition forces. As one academic study concluded, protection payments in connection with “development projects and supply contracts” thus “fund[ed] the Taliban and their affiliates” while also “encouraging alienated men to join the insurgency for easy money.”³⁰²

941. This financial link applied to protection payments in all their forms. Due to the Taliban’s fundraising apparatus, cash payments to local commanders (or the Taliban Financial Commission) flowed to Taliban leadership for use wherever the insurgents decided to focus their resources. “Salary” payments to Taliban fighters had a similar effect. Not only did those payments relieve financial pressure on local Taliban commanders, but the Taliban extracted a portion of all salary payments received by individual Taliban members – which it likewise routed to the Taliban Financial Commission for the benefit of the nationwide insurgency.

942. Protection payments supplied one of the most quantitatively significant sources of funding for the Taliban. As Secretary of State Hillary Clinton testified before the U.S. Senate Committee on Foreign Relations in 2009: “[O]ne of the major sources of funding for the Taliban is the protection money.”³⁰³ The systematic payments effected by large international companies swamped other, smaller-scale protection rackets. “A far larger source of Taliban income” as compared to such other schemes, the *Sunday Telegraph* reported in September 2009, was the

³⁰¹ *Meyer Interview*.

³⁰² *Economic Impediments* at 80.

³⁰³ *Afghanistan: Assessing The Road Ahead*, Hr’g Before the U.S. Senate Committee on Foreign Relations, S. Hr’g 111-479, at 48 (Dec. 3, 2009) (statement of Hillary Rodham Clinton, Sec’y of State, U.S. State Dep’t) (“S. Hr’g 111-479”).

money the Taliban extracted from companies providing security or “provid[ing] new infrastructure, such as schools and roads.”³⁰⁴ The Commission on Wartime Contracting thus concluded that “[e]xtortion of funds from U.S. construction projects and transportation contracts is the insurgents’ second-largest funding source,” behind only drug trafficking.³⁰⁵

943. In many areas of the country, protection payments supplied the single most significant source of funding for insurgent violence. In areas where “there [wa]s little or no poppy grown,” protection rackets were “believed to be the largest source of income for the insurgents.”³⁰⁶ That was nowhere more true than in the areas where the Taliban acted through the Haqqani Network. In the areas of Haqqani influence – including eastern and southeastern provinces where many Defendants did business – protection money accounted for “the network’s largest source of income.”³⁰⁷ As one local businessman with experience in the area reported of the Haqqanis, “Compared to extortion, . . . everything else is peanuts.”³⁰⁸

944. Protection payments also strengthened the Taliban by allowing it to diversify its income. For an insurgent group subject to crippling international sanctions, diversification was critical: it offered the Taliban a degree of financial resiliency that made it less susceptible to American counterinsurgency efforts. That is why, as the U.S. military began to successfully interdict the Taliban’s other revenue sources (such as narcotics), the Taliban relied increasingly

³⁰⁴ Christopher Booker, *How We Help To Arm The Taliban*, Sunday Telegraph (Sept. 13, 2009) (“*How We Help To Arm The Taliban*”).

³⁰⁵ *CWC Report* at 74. As additional evidence surfaced, it became clear that the “drug trade” was not “as big a funding source for the insurgency as a lot of people thought.” *Meyer Interview*. Rather, U.S. intelligence surfaced evidence that U.S. government-funded “development projects” became “one of the biggest funding sources for the insurgency.” *Id.*

³⁰⁶ *Crime & Insurgency* at 31.

³⁰⁷ *Haqqani Network Financing* at 40.

³⁰⁸ *Id.*

on its protection rackets. That stream of protection money – particularly from larger, well-financed contractors, including Defendants – supplied reliable funding for the insurgency and, almost as importantly, offered insurance against the risk of other funding sources drying up.

945. Protection payments from Western companies, including Defendants, were also qualitatively material to the Taliban’s terrorist enterprise because of their unique link to the Taliban’s leadership. Unlike funding from other sources (such as smaller businesses) that were more often spent locally, Defendants’ protection payments generally flowed up the Taliban’s organizational chain – or were made directly to top-level Taliban institutions – and supplied fungible U.S. dollars available for use by leadership wherever it saw fit.³⁰⁹ In addition, the payments often conferred intelligence benefits to the Taliban by providing details about U.S. government, military, and contractor operations in the area. The Taliban’s high-level commanders then used the money and intelligence supplied by Defendants to finance their nationwide terrorist campaign against Americans in Afghanistan.

946. The Taliban’s top-down organizational hierarchy ensured that protection money collected locally in one province helped to finance Taliban operations throughout the country – including in provinces miles away from the site of the payment. That was a core reason why the Taliban moved to institutionalize the collection of protection money from large firms, including Defendants: rather than have commanders spend their protection money locally, the Taliban directed the funds into the group’s central coffers for use on a nationwide scale.³¹⁰ As two Afghanistan scholars documented, such “funds flow[ed] from Taliban-controlled regions up the

³⁰⁹ *Id.* ¶ 35 (“[T]he money flowing from “construction and trucking companies, mobile telephone operators, mining companies[,] and aid and development projects goes to the Taliban Financial Commission[,] which answers to the Taliban leadership.”).

³¹⁰ *See id.*; *Crime & Insurgency* at 17.

chain of command to the leadership and then bec[a]me re-dispensed in the form of individual payments” in key provinces throughout Afghanistan.³¹¹ Accordingly, Defendants’ payments did not merely finance attacks in the immediate areas of their projects; the Taliban’s process for redistributing those payments made sure that they financed terrorism throughout Afghanistan.

2. Defendants’ “Free Goods” Protection Payments To The Taliban, Including Its Haqqani Network, Directly Funded, Armed, And Logistically Supported Al-Qaeda And Taliban, Including Haqqani Network, Attacks Against Americans In Afghanistan

947. Defendants’ provision of free communications technologies to the Taliban, including its Haqqani Network, as a form of “free goods” protection payments to the terrorists furthered the IRGC’s Conspiracy and provided critical aid to al-Qaeda and the Taliban. At all times, Defendants were aware of the key role that communications technologies played in propagating attacks against Americans by al-Qaeda and its allies. As Eric Schmidt, then Google’s Chair and CEO, and Jared Cohen, then the Director of Google Ideas, noted in 2010:

[F]or all the inspiring stories and moments of hope abetted by the use of connection technologies, the potential of such technologies to be manipulated or used in dangerous ways should not be underestimated. The world’s most ... violent transnational groups—from al Qaeda ... to the ... Taliban—are effectively using technology to bring on new recruits, terrify local populations, and threaten democratic institutions. ... The same encryption technologies used by dissidents and activists to hide their private communications and personal data from the state are used by would-be terrorists... Afghanistan’s telecommunications networks provide a useful case study in how connection technologies can both help and harm a nation. Since U.S. and NATO forces first launched military operations there in 2001, cell-phone access in Afghanistan has grown from zero to 30 percent. ... At the same time, the Taliban have become increasingly savvy about using mobile technology to malicious and deadly effect. Taliban militants have used cell phones to coordinate attacks, threaten local populations, and hold local businesses hostage ... In February 2009, Taliban inmates in Kabul’s Policharki prison used cell phones to orchestrate a number of coordinated attacks on Afghan

³¹¹ *Economic Impediments* at 75.

government ministries. In Afghanistan—and Iraq, too—it is not uncommon for insurgents to use cell phones to detonate roadside bombs remotely.³¹²

948. Defendants’ “free goods” deliveries of cell phones, including phones manufactured and/or acquired in the United States, to the Taliban, including its Haqqani Network, also provided another direct cash equivalent, worth approximately \$2,000 per cell phone, to al-Qaeda and the Taliban, including its Haqqani Network. Indeed, at all times, the high-tech cell phones that Defendants illicitly sourced for, and furnished to, the Taliban, including its Haqqani Network, as a “free goods” form of protection payment to such terrorists, carried unique value in Afghanistan that ensured their status as one of the single most valuable items any person, including any terrorist, could possess. As the *Sydney Morning Herald* explained, from 2004 onward, “[c]ommunications [were] vastly better” in Afghanistan and, as a result, “Afghans who [could] afford a mobile phone *clutch[ed] them like talismans*; even the Taliban spokesman avail[ed] himself of the best technology: a satellite phone with an automatic message bank that respond[ed] in 10 languages.”³¹³

949. Defendants’ “free goods” deliveries of cell phones, including phones manufactured and/or acquired in the United States that Defendants illicitly sourced from America, to the Taliban, including its Haqqani Network, also aided the terrorists’ fundraising campaigns because it gave the Syndicate the technical tools they required to send communications to others requesting (or demanding) payments, including, but not limited to, sending text messages to Afghans soliciting *zakat* contributions and sending messages to

³¹² Eric Schmidt and Jared Cohen, *The Digital Disruption: Connectivity and the Diffusion of Power*, Foreign Affairs, Vol. 89, Issue 6 (Nov. 1, 2010), 2010 WLNR 28476557.

³¹³ Paul McGeough, *In the Shadow of the Guns*, *Sydney Morning Herald* (Aug. 27, 2005), 2005 WLNR 28183961.

companies, including Defendants, soliciting protection payments or, if such terms were already agreed upon, reminding that a payment was due.³¹⁴

950. Defendants’ “free goods” deliveries of cell phones, including phones manufactured and/or acquired in the United States that Defendants illicitly sourced from America, to the Taliban, including its Haqqani Network, also provided direct operational and logistical support to al-Qaeda and the Taliban, including its Haqqani Network, by furnishing untraceable, valuable, cell phones, which the terrorists could use to communicate with one another to securely coordinate smuggling, transportation, attack plans, and the like.

951. Defendants’ “free goods” payments of free cell phones to the Taliban, including its Haqqani Network, allowed the Syndicate to maintain its cell phone stockpile without spending as many previous U.S. Dollars to do so, providing the terrorists a substantial logistical and financial windfall. In 2006 the *Independent* reported on the common experience, reflected by the example of an Afghan’s experience in a key district (Panjawi) in the Taliban’s stronghold of Kandahar, that “the Taliban in his district [had] little money but they ha[d] mobile phones.”³¹⁵

952. Moreover, like its IRGC sponsors, al-Qaeda, the Taliban, and their Syndicate allies in Afghanistan and Pakistan depended upon a vast stockpile of cell phones in order to

³¹⁴ See, e.g., Rachel Ehrenfeld and John Wood, *Funding Terror; New Technology Terrorists Can Use*, Wash. Times (Mar. 15, 2007) (“We are on the cusp of a new era of terror financing, that of mobile payments or ‘m-payments.’ ... Are Hamas, al Qaeda, Hezbollah and their likes far behind? Soon, every mobile-phone owner will be able to send money, pay bills and make purchases anywhere, anytime. ... Without the implementation of a real-time digital anti-money-laundering compliance framework, the m-payment system is well suited to become the ‘killer application’ for money laundering and terror financing. All you need is a stored value card and m-payments enabled mobile phone and carrier ... [for] members of Hamas and Hezbollah in the United States to send money back to the Middle East, or to each other all over the world ... [including in areas like] Dubai[,] ... a well-known conduit for al Qaeda, Hamas and Hezbollah funding.”), 2007 WLNR 4912741.

³¹⁵ Nelofer Pazira, *Taliban’s Terror Tactics Reconquer Afghanistan*, *Independent* on Sunday (UK) (August 20, 2006), 2006 WLNR 17604097.

conduct their terrorist enterprise in Afghanistan, Pakistan, the U.A.E., Iran, and the other key geographies worldwide from which al-Qaeda and the Taliban facilitated terrorist attacks against Americans in Afghanistan. When Defendants provided more than 1,000 “free” cell phones each year, they furnished a key supply of untraceable phones to the terrorists that aided their communications, attack planning, attack operations, logistics, propaganda, smuggling, and travels – every facet of the terrorists’ enterprise targeting Americans in Afghanistan.

953. Al-Qaeda alone, for example, required tens of thousands of untraceable mobile phones each year for the thousands of operatives it deployed in Afghanistan and Pakistan in support of the attacks. For example, in 2002, media accounts noted that “[t]housands of al Qaeda members hiding in Pakistan use[d] cell phones,”³¹⁶ while, “[i]n Afghanistan, al Qaida were using top-of-the-range cellular phones,”³¹⁷ both of which trends always endured.

954. Defendants’ “free goods” payments of free cell phones to the Taliban, including its Haqqani Network, also armed al-Qaeda and the Taliban because Defendants’ free phones were, themselves, weapons when wielded by Syndicate terrorists. By 2008, while “cell phone[s]” were “[n]othing special in America,” cell phones were “having a profound effect in Afghanistan[,]” where “[m]any Afghans now rel[ied] on cell phones, as [did] Taliban militants.”³¹⁸ As the *Associated Press* reported at the time, “Taliban” “militant fighters rely on mobile phones to communicate and coordinate their operations.”³¹⁹

³¹⁶ Ralph Joseph, *Chemical Labs Show Al Qaeda Still Active*, Wash. Times (Oct. 6, 2002), 2002 WLNR 383410.

³¹⁷ Phil Hazlewood and Tom Whitehead, *Role of Aircraft Patrolling Skies*, PA News (Feb. 13, 2003).

³¹⁸ NPR Morning Edition, *Cell Phones Connect Afghans to Rest of World* (Feb. 26, 2008), 2008 WLNR 3764701.

³¹⁹ Noor Khan, *Taliban Destroy 2 Phone Towers in Southern Afghanistan*, AP DataStream (Mar. 2, 2008).

955. Al-Qaeda and the Taliban also used deployed some of Defendants’ “free goods” donations of cell phones as part of their IEDs, using the phones to detonate the bombs that killed Americans in Afghanistan, including on information and belief many Plaintiffs.³²⁰ By 2005, “[i]t [was] an irony of the digital age that technology ha[d] aided the security forces in detecting and thwarting terrorist operations ... helped terrorists do their evil.”³²¹ “High-tech communication” technologies, including “[c]ell phones,” in the hands of an al-Qaeda operative after 9/11, constituted a “weapon at the disposal of” the al-Qaeda “terrorist” because “[c]ell phones” “were a key in” Al-Qaeda’s ability to execute “coordinated attack[s],” including “suicide terrorist attack[s],” which attacks were “facilitated by” al-Qaeda’s access to “hi-tech communications” technologies, including “[c]ell phones.”³²² Moreover, when the Syndicate’s IED campaign intensified in 2009-2010, so did its reliance on cell phones, which remained a key detonator.³²³

956. Defendants’ “free goods” payments of free cell phones to the Taliban, including its Haqqani Network, also directly facilitated communications between forward deployed al-Qaeda and Taliban, including Haqqani Network, terrorists in Afghanistan and their leadership in

³²⁰ See, e.g., AllAfrica.com English, *Terrorists Drew World’s Attention in Madrid* (Apr. 2, 2004) (“Technology has also linked al-Qaeda to the Madrid bombings. Al-Hayat claims that an Islamist source revealed to the newspaper that al-Qaeda trained its fighters in Afghanistan to use mobile phones for setting off explosive devices. The source told al-Hayat that the explosions on the trains were triggered by mobile phones with alarm clocks set to go off at a specific time.”).

³²¹ James D. Zirin (Member, Council on Foreign Relations), *Terrorism in the Digital Age*, Wash. Times (Dec. 6, 2005), 2005 WLNR 19631068; United News of Bangladesh, *Bomb at Pakistan Shiite Procession Kills 7* (Nov. 24, 2012) (“Officials say Taliban frequently use cellular phones as remote detonators for bomb attacks.”).

³²² *Id.*

³²³ See, e.g., CNN Newsroom, *Goes Green; Updates on Major Accident on Missouri’s I-44 Crash - Part 1*, AP Alert – Environment (Aug. 6, 2010) (CNN reporting that “the Taliban us[ed] IEDs in a deadly campaign of intimidation against Afghan villagers,” the Taliban’s “IEDs” were “the top killers of American and coalition forces,” “often made of cheap materials like fertilizer” and “detonated by” “something as simple as a cell phone”).

Pakistan, which accelerated the pace of the Syndicate's attack planning and logistics-related communications, causing more al-Qaeda and Taliban attacks against Americans in Afghanistan. Defendants' free cell phones were vital because, given the nature of communications between Afghanistan and Pakistan, "telecommunication" technologies were "[t]he only way" that "Taliban commanders" at "Taliban headquarters in Pakistan" could communicate with "Taliban" "field commanders in Afghanistan and outside actors in" other countries,³²⁴ e.g., the IRGC.

VIII. DEFENDANTS KNEW THAT THEIR TRANSACTIONS WITH HEZBOLLAH, THE QODS FORCE, REGULAR IRGC, AL-QAEDA, AND THE TALIBAN, INCLUDING ITS HAQQANI NETWORK, FACILITATED EVERY NODE OF THE CONSPIRACY AND DIRECTLY AIDED TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN

A. Defendants Knew Their Transactions With Hezbollah, Qods Force, And Regular IRGC Fronts, Operatives, Agents, And Cut-Outs Furthered The IRGC's Conspiracy To Attack Americans In Afghanistan

957. Defendants knew that their transactions with fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC financed, armed, and operationally supported Iranian proxy terrorist attacks against Americans in Afghanistan.

958. Defendants knew that "[c]ompanies doing business in Iran face substantial risks..., ' said Sigal Mandelker, Treasury Department undersecretary for terrorism. She added:

.... "deceptive" Iranian transactions that ultimately channel money to terrorists. The Iranian government "uses shell and front companies to conceal its tracks" as part of an elaborate scheme designed to procure cash for the Quds Force of Iran's militant Islamic Revolutionary Guard Corps, which the U.S. designates as a terrorist organization.

959. By early 2005, it was widely understood in diplomatic, business, and military circles that Hezbollah, the Qods Force, and Regular IRGC had seized control of Iran's telecom,

³²⁴ Stewart Bell, *Canada Listening In On Taliban Exchanges*, National Post (May 1, 2007), 2007 WLNR 28591271.

communications, and information technology sectors. Before they transacted with IRGC, including Hezbollah and the Qods Force, fronts, operatives, and agents, Defendants were aware that IRGC, including Hezbollah and the Qods Force, had seized control of these sectors.

960. Defendants were aware of IRGC's capture of Iran's telecom, communications, and information technology companies in part through their local agents and affiliates, whom Defendants relied upon to keep abreast of Iranian market conditions; these agents (who were subject to Defendants' control and whose knowledge is imputed to Defendants) knew that Hezbollah, the Qods Force, and Regular IRGC controlled Iran's telecom, communications, and information technology sectors and used that control to raise money, obtain weapons, and source operational support for terrorism. As a general matter, those agents spoke fluent Farsi, had relationships with people throughout Iranian government and industry, and were well-informed about Iranian politics and economics. They could not have remained ignorant of the common understanding that the Iranian telecom, communications, and information technology sectors were controlled by Hezbollah, the Qods Force, and Regular IRGC.

961. Defendants knew, or recklessly disregarded, Hezbollah, the Qods Force, Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, routinely used commercial transactions to raise money and acquire key weapons and weapons components in support of the IRGC's lead terrorist agent, Hezbollah, as well as the IRGC's proxies in Afghanistan, al-Qaeda and the Taliban. As a regional studies professor explained, "Dubai ... maintains crucial avenues for the IRGC ... to generate money" and serves as "the gate to the world for" Iranian terrorist front company efforts.³²⁵

³²⁵ TRT World (Turkey), *Amid Soleimani Crisis, Iran Threatens to Level Dubai and Israel. But Why?* (Jan. 8, 2020), 2020 WLNR 663153.

962. Defendants knew, or recklessly disregarded, that as American sanctions sought to choke off IRGC, including Hezbollah and the Qods Force, access to the global financial system escalated, Hezbollah, the Qods Force, and Regular IRGC responded by using IRGC, including Hezbollah and the Qods Force, front companies and agents in the United Arab Emirates, Iraq, and elsewhere to raise money through criminal enterprise, facilitate terrorist finance through the banking system, and maintain the steady supply of key telecom, communications, and information technologies necessary to continue to prosecute a terrorist campaign against Americans in Afghanistan and elsewhere. Per *Reuters*, the IRGC:

long proved successful in defending [its] economic interests, including in recent years when the sanctions ... effectively exclude[ed] Iran from the global financial and trading system. “Even under very difficult economic circumstances, the funds for the IRGC’s activities, whether domestic or overseas, remained intact,” said a former official close to the [Iranian] government... As the U.S. and EU sanctions on Iran’s oil and finance sectors in 2012 started to bite, the [IRGC] responded by setting up complex operations involving the likes of Dubai ***“The IRGC started to buy hundreds of ... companies around the [U.A.E.] to use as front companies,”*** said a trader involved in ... the oil industry. ***“These companies partnered with some foreign companies to bypass sanctions. Most of the time cash was delivered to a foreign account in a neighbouring country.”***³²⁶

963. At all relevant times, Defendants understood that the U.S. government believed that IRGC, including Hezbollah and the Qods Force, activities in the U.A.E. supported anti-American terrorism in Afghanistan and Iraq. For example, in 2008, President George W. Bush gave a widely-reported speech to U.A.E. government and business leaders in which he called Iran “the world’s leading sponsor of terrorism” and stressed that illicit transactions in the U.A.E. were important to the IRGC’s, including Hezbollah’s and the Qods Force’s, ability to provide “support for Islamist groups and militants in Afghanistan, Iraq, Lebanon and the Palestinian

³²⁶ Parisa Hafezi, *RPT-INSIGHT-Iran’s Elite Guards to Gain Regional, Economic Power in Post-Sanctions Era*, Reuters News (Jan. 20, 2016) (emphasis added).

territories.”³²⁷ Press reports concerning President Bush’s speech emphasized the U.S. government’s efforts “to enforce US sanctions against ... the Quds Force of the IRGC” because “Dubai in particular ha[d] become a financial centre handling substantial Iranian investments which the administration want[ed] to restrict.”³²⁸

964. From 2005 through 2016, accounts from prominent Western media sources also reported on the direct link between the Iranian telecom, communications, and information technology sectors and Hezbollah, the Qods Force, and Regular IRGC.

965. On information and belief, Defendants were aware of these reports documenting the link between their Iran-related counterparties and Hezbollah, the Qods Force, and Regular IRGC. Each Defendant generally maintained a corporate security group responsible for supervising their global supply chains, doing counterparty diligence, and preventing the theft or diversion of the devices or services they sold, including in the Middle East. As part of such efforts, Defendants’ standard practice would have been to conduct basic open-source research on the Iranian telecom market and the mechanics of making telecom deals in Iran – even a modicum of which would have uncovered the reports discussing the Iranian front entities’ terrorist ties set forth above.³²⁹

³²⁷ APS Diplomat Redrawing the Islamic Map, *Bush Says Iran Poses Threat To Global Security* (Jan. 14, 2008), 2008 WLNR 25283869.

³²⁸ *Id.*

³²⁹ This allegation applies to all Defendants except MTN Irancell. Plaintiffs allege that MTN Irancell relied upon Hezbollah, the Qods Force, and Regular IRGC to conduct diligence on the counterparties with whom MTN Irancell conducted business, and that the IRGC, including Qods Force, fronts, operatives, and agents that owned and managed MTN Irancell would not have approved any significant investment or hire by MTN Irancell if Hezbollah, the Qods Force, and Regular IRGC believed that such proposed deal did not benefit the “security” agenda of the IRGC, including Hezbollah and the Qods Force.

966. After 2005, Defendants could not have conducted credible due diligence that would have “cleared” their transactions with their counterparties controlled by Hezbollah, the Qods Force, and Regular IRGC. Defendants also knew that the IRGC’s, including Hezbollah’s and the Qods Force’s, control of their business partners based upon the statements set forth in prominent due diligence materials concerning Iran.

967. MTN’s collusion against Turkcell with the conservatives who controlled Hezbollah, the Qods Force, and Regular IRGC fronts responsible for the Irancell contract itself became a notable “red flag” about the highly risky Iranian business environment that Defendants knew of—and ignored. For example, as the *Economist*’s flagship due diligence report, the *Economist Intelligence Unit*, explained in June 2005:

There is considerable doubt that [] Turkish investment projects ... will proceed after facing opposition from the new conservative-dominated [Iranian parliament, the] Majlis. The Majlis in late 2004 passed a law giving it a veto over foreign investment and in early 2005 ruled that Turkcell ... should reduce its stake in [] Irancell ... to 49% from 70% [and] ... that a majority of Iranian shareholders would have to support any management decisions and that security issues be referred to the intelligence ministry and the Supreme National Security Council. ... The Majlis’s opposition to the projects ... is sure to cause nervousness among foreign investors who will see it as calling into question the value of contracts in the Islamic Republic and as a sign of arbitrariness in governance.³³⁰

968. After MTN had finished off Turkcell and secured the Irancell license from Hezbollah, the Qods Force, and Regular IRGC fronts who controlled Irancell, the *Economist* updated its standard diligence briefing concerning Iran to warn potential investors, including Defendants, against the “High Risk” of doing business with Iranian entities:

Foreign investors are deterred by the nationalist stance of the Majlis towards foreign investment (High Risk). The Majlis in late 2004 passed a law giving it a veto over foreign investment which it has used to ... severely tighten up on the terms of a project by Turkcell ... ***The conditions imposed on Turkcell have seen***

³³⁰ Economist Intelligence Unit, *Iran Risk: Legal & Regulatory Risk*, Risk Briefing (June 29, 2005), 2005 WLNR 26571496.

its bid superseded by a South African company, MTN. The episodes caused nervousness among foreign investors who fear that they called into question the value of contracts in [Iran] and indicated arbitrariness in government decision-making. President Mahmoud Ahmadinejad's presidency (until at least 2009, when fresh elections will take place) will *continue to heighten such concerns*. ...³³¹

969. Public statements made by prominent Members of Congress also alerted Defendants to the IRGC's control of the Iranian telecom sector. For example, on February 10, 2011, a bipartisan group of United States Senators and Representatives confirmed the widespread understanding that the IRGC's (and by extension, the Qods Force's) control of the "Iran telecom sector, of which the Iranian Revolutionary Guard Corps owns a significant stake."³³² These Members' letter received widespread coverage in the global media.

970. Pressure campaigns, also known as "private sanctions," by public interest groups also warned Defendants about the IRGC's control of the Iran telecom sector. For example, from 2011 through the present, the non-partisan group UANI³³³ has pressured technology and telecom companies to cut ties with IRGC, including Hezbollah and the Qods Force, fronts in order to

³³¹ Economist Intelligence Unit, *Iran Risk: Legal & Regulatory Risk*, Risk Briefing (Nov. 9, 2006) (emphasis added), 2006 WLNR 26677912.

³³² Letter from U.S. Senators Jim Webb, Jon Kyl, and Richard Burr, and U.S. Representatives Ileana Ros Lehtinen and Sue Myrick, *Sens. Webb, Kyl: Sale of U.S. Computer Technology to Chinese Firm Poses Serious Risk Chinese Firm Has History of Illegal Behavior and Ties with the People's Liberation Army, Taliban and Iranian Revolutionary Guard*, States News Service (Feb. 10, 2011).

³³³ UANI is a non-partisan group that focuses on protecting American national security from the threat posed by Iran. In 2012, UANI and its Advisory Board included an array of former national security officials from the U.S. U.K., Germany, Israel, and others, including "Graham Allison, Les Gelb and Fouad Ajami, and former government officials including former CIA Director Jim Woolsey, former Homeland Security Advisor Fran Townsend, former Mossad Chief Meir Dagan, former head of the German Intelligence Service Dr. August Hanning, and former head of the United Kingdom's MI6 Sir Richard Dearlove among many others." Wallace May 17, 2012, Testimony.

pressure the Iranian regime to cease its support for anti-American terror and other malign activities in the Middle East. As Ambassador Mark D. Wallace explained in 2012:

[I]n 2011 UANI launched its “Tech and Telecom Campaign” to ***publicly highlight the role of telecommunications companies in Iran and about how their technology was being misused by Iranian government security forces*** ... In so doing, companies were ***directly facilitating the ability of the Iranian regime to wage a campaign of terror*** ... In response to UANI’s campaign, companies like Nokia Siemens Networks and Ericsson agreed to not take on any new business in Iran. ... In today’s integrated business and financial worlds, companies cannot exist in a national vacuum. Any corporation that seeks access to American capital [] is subject to American law, public pressure and American public opinion.³³⁴

971. Defendants also knew that most of their multinational peers had already chosen to exit ventures in which they participated alongside Iranian entities that could potentially be fronts for Hezbollah, the Qods Force, and Regular IRGC. By 2012, the roster of companies that announced an intention to depart Iran included such prominent multinationals as Siemens, Ingersoll Rand, Hitachi, ABB, Porsche, Caterpillar, Komatsu, Bobcat, and others. Huawei was one of the companies to announce its intentions to depart Iran as well, but as alleged herein, Huawei actually did not pull out of the Iranian market. Regardless of whether Defendants’ other multinational peers, in fact, exited these Iranian relationships, their public announcement of their intention to do so further alerted Defendants to the extreme risk posed by their continued economic relationships with their Iranian counterparties.

972. On April 24, 2016, the *Washington Post* published an opinion written by Senator Joseph I. Lieberman, and Amb. Mark D. Wallace in which the authors warned multinational corporations of the severe financial and reputational risk attendant to doing business with a notorious IRGC front, like MTN Irancell, presciently warning Defendants that, “[s]evere risks exist for companies thinking about investing with the ayatollah, including doing business with

³³⁴ Wallace May 17, 2012, Testimony (emphasis added).

the wide array of front companies tied to the IRGC, a terrorist organization sanctioned by the United States and the international community.”³³⁵

973. MTN, from at least 2005 through the present, ZTE, from at least 2008 through at least 2016, and Huawei, from at least 2008 through at least 2014, knowingly structured their transactions to facilitate the IRGC’s fundraising, weapons procurement, and operational support from their IRGC-controlled, including Hezbollah- and Qods Force-controlled, counterparties – which Hezbollah, the Qods Force, and Regular IRGC used to support, among other things, al-Qaeda’s and the Taliban’s terrorist attacks against Americans in Afghanistan. Senior Iranian entity officials involved in the Defendants’ transactions were avowed, well-known fronts, operatives, and agents for Hezbollah, the Qods Force, and Regular IRGC.

974. On information and belief, the ZTE, Huawei, and MTN Co-Conspirators extensively collaborated in Iran, by sharing U.S.-origin technology between 2007 and the present day. As early as 2004, MTN Group created a UK-based shell company called Surizon. Surizon’s co-owners, its CEO, and “head of international business development” were previously members of MTN Group’s founding board, including its General Counsel and the architect of its international expansion.

975. Surizon’s primary products were two software applications: Fast Access to Content, Trends and Statistics (“FACTS”) and Network Management System (“NMS”). FACTS was, and still is, an “intelligence system.” NMS enables companies to manage and monitor networks like Irancell’s and TCI’s mix of incompatible US, European, and Chinese-supplied hardware to enable them to supply meaningful data to FACTS.

³³⁵ Sen. Joseph I. Lieberman (I-NY) and Amb. Mark D. Wallace, *Why Iran Is Arming Up*, Washington Post (Apr. 24, 2016).

976. According to statements by Surizon and multiple MTN and Irancell employees, Surizon's products were, in essence, interfaces and data manipulation scripts wrapped around U.S.-origin technologies created by, *inter alia*, Oracle, Roambi, and BMC. On information and belief, between 2006 and 2007, Surizon and MTN Group 'negotiated' a "21-country deal" to provide "FACTS... across all MTN Group operators."

977. Surizon and MTN Group customized and deployed FACTS and NMS to each and every one of MTN Group's operating companies, including Sudan, Syria, and Iran, and specifically including the companies whose facilities are integrated into Iran's transnational signals intelligence network.

978. On information and belief, MTN continues to use and share FACTS and NMS software with third parties, including the Huawei and ZTE Defendants.

979. The U.S.-origin technologies used by MTN Irancell and supplied by MTN to Huawei and ZTE, and through Huawei and ZTE to TCI, enabled IRGC, including Hezbollah and the Qods Force, to collect surveillance data and deliver intelligence in real time to terrorist agents in the field via smart phone applications. Use of the U.S.-origin technology, as provided by MTN, Huawei, and ZTE, allowed the terrorists to monitor, track, and target Americans. Indeed, the U.S.-origin technologies enabled FACTS users and Iranian third parties to receive text message alerts under user-specified conditions, and to access network data, including interactive maps of subscriber activity using their smart phones, and to query and mine the data its network operations centers collected, via ZTE and Huawei-supplied surveillance hardware (which themselves were also based on U.S.-origin technologies).

980. On information and belief, MTN provided ZTE, Huawei, and their Iran-based subsidiaries and shell companies with access to Surizon-developed software to realize a

partnership in which ZTE and Huawei provided hardware to MTN-Irancell and managed its network operations centers, including those co-located with Iranian intelligence agents, on a day-to-day basis.

981. On information and belief, MTN also provided FACTS to TCI and MCI, and to its local Iranian partners, as well as to agents of Hezbollah, the Qods Force, and Regular IRGC. FACTS and NMS enabled the partnership to manage its highly complex multi-vendor network, and to collaborate seamlessly, avoiding serious compatibility issues that would have arisen from using their own in-house applications.

982. Defendants knew or recklessly disregarded that their corrupt transactions, overseen by a counterparty that Hezbollah, the Qods Force, and Regular IRGC had totally commandeered, delivered resources directly to Hezbollah, the Qods Force, and Regular IRGC which they provided to al-Qaeda and the Taliban, including its Haqqani Network, in the form of funds, weapons, logistical support, and other aid to commit terrorist attacks against Americans in Afghanistan by al-Qaeda and the Taliban.

983. The IRGC's control over the Iranian telecom, communications, and computer sector was so complete that by 2004, there was no longer any meaningful distinction between any of the large Iranian telecom, communications, or computer companies and Hezbollah, the Qods Force, and Regular IRGC. Because Hezbollah, the Qods Force, and Regular IRGC had effectively captured the Iranian telecom, communications, and computer sectors and was using such control to fund and arm IRGC proxies that led the al-Qaeda and Taliban attacks against Americans in Afghanistan, transactions with Iranian telecom, communications, and information technology companies directly benefited the Afghanistan Terror Campaign.

984. Defendants’ transactions with their IRGC-controlled, including Qods Force-controlled, Iranian counterparties supplied Hezbollah, the Qods Force, and Regular IRGC, and through such IRGC members, al-Qaeda and the Taliban, including its Haqqani Network, with resources critical to the Syndicate’ terrorist operations against Americans in Afghanistan. The IRGC’s control over these critical Iranian economic sectors – and the enormous cash flow that came with it, both from normal revenue as well as corrupt payments from foreign companies – was a key source of the IRGC’s, including Hezbollah’s and the Qods Force’s, power.

985. Indeed, the telecom, communications, and information technology sectors were (and remain) controlled by Hezbollah, the Qods Force, and Regular IRGC precisely because such control allows Hezbollah, the Qods Force, and Regular IRGC to make groups like Hezbollah more effective at attacking the enemies of Iran, both foreign and domestic, through the substantial funding for Hezbollah, the Qods Force, and Regular IRGC which flows through to IRGC proxies, including al-Qaeda and the Taliban. The IRGC’s complete conversion of the telecom, communications, and computer sectors of the Iranian economy as direct tools of terrorism further strengthened the potency of Defendants’ illicit transactions as a means of financing, arming, and operationally supporting attacks.

986. Defendants provided fungible funds to Hezbollah, the Qods Force, and Regular IRGC that inevitably flowed through to, among others, al-Qaeda and the Taliban for attacks against Americans in Afghanistan. As Ambassador Mark D. Wallace explained in 2012, “[a]bsent *economic support from international businesses*, the Iranian regime would *not have the financial wherewithal to ... support terrorism*.”³³⁶

³³⁶ Wallace May 17, 2012, Testimony (emphasis added).

987. Writing in the *Eurasia Review*, a foreign affairs analyst specializing in Iran explained the tight nexus between economic transactions with the Bonyad Mostazafan and Hezbollah-supported terrorist attacks against Americans in the Middle East:

The question is, where does the revenue go? ... Since US sanctions caused a sharp decline in Iran's official revenues, the regime is facing financial difficulties and cannot fund its proxies to meddle in the region or as the mullahs' call it "expand its strategic scope". ***Iran cannot fund its proxies including Hezbollah, and its multitude of militia forces in Iraq*** and Yemen, or its Afghan Fatemiyoun Division and Pakistani Zainebiyoun militias in Syria using its official annual budget. ***The millions of dollars used to fund these group must be provided from other financial sources.*** ...[B]onyads such as Bonyad-e-Mostazafan, are among the organizations that have ***directly assisted the Quds Force in this regard.*** Iranian opposition sources have previously stated that the Quds Force receives ***most of its funds*** from [Bonyads]. ... The US's decision to sanction [Bonyads] will definitely be welcomed by Iranians who are tired of having their ***stolen wealth used for terrorism.***³³⁷

988. Juan C. Zarate, former Deputy National Security Advisor for Combatting Terrorism from 2005 through 2009, previously testified about the key role played by IRGC, including Hezbollah and the Qods Force, front companies in funding and arming anti-American terrorist attacks committed by Iranian terrorist proxy groups:

We have limited tools to address ... terrorism ... And the use of financial power and the power to exclude from the global system is one of our principal if not most effective tools [W]e have to have a comprehensive strategy with the use of all tools of national power. No doubt. But the reality is at the end of the day, these tools are the ones that prove to be most effective.... So we are going to have to, ***if we are honest about what's happening in the international financial commercial order, we are going to have to crack down on Qods Force front companies.***.... That's the nature of the Iranian economy in the way that they do business, and the way they have reached precisely what we have cut off that hardened them so much.³³⁸

³³⁷ Cyrus Yaqubi, *Recently Sanctioned Iran Foundation Is Regime's Slush Fund For Terrorism*, *Eurasia Review* (Jan. 24, 2021) (emphasis added). While Mr. Yaqubi primarily focused on a separate bonyad, his claims apply equally to Bonyad Mostazafan. *See id.* ("[B]onyads such as Bonyad-e-Mostazafan, ... have directly assisted the Quds Force in this regard.").

³³⁸ Testimony of Juan Zarate, *Sen. Bob Corker Holds a Hearing on Sanctions and the Joint Comprehensive Plan of Action*, SEC Wire (July 31, 2015) (emphasis added).

989. On April 23, 2012, the Treasury Department announced new sanctions against Iran that recognized that the IRGC's control of the telecommunications sector was inextricably linked with violence, and stated, in part, as follows:

The Order targets ...information and communications technology that facilitates computer or network disruption, monitoring or tracking that could assist in or enable human rights abuses by or on behalf of the ... Government of Iran. Pursuant to this order sanctions were imposed on ... Iran's Islamic Revolutionary Guard Corps (IRGC) ... The IRGC's Guard Cyber Defense Command (GCDC) includes a special department called the Center for Inspecting Organized Crimes (CIOC). ... The IRGC's CIOC has openly admitted that it would forcefully suppress anyone seeking to carry out "cultural operations" against the Islamic Republic via the Internet ... Individuals arrested by the IRGC have been subjected to severe mental and physical abuse³³⁹

990. The nexus between Defendants' illicit transactions in the Iranian telecom sector and terrorist violence by Iranian proxies was especially tight. As Ali Alfoneh of the American Enterprise Institute explained, Hezbollah, the Qods Force, and Regular IRGC pushed their way into the telecom sector mafia-style, and relied upon the funds and technology they acquired through their telecom front companies to fund IRGC, including Hezbollah and the Qods Force, operations:

Telecommunications

The *IRGC has also muscled its way into the Iranian telecommunications sector*. In February 2002, Turkish cell phone company Turkcell ... won a bid to inaugurate a second mobile phone network for Iran ... *The Iranian government welcomed Turkcell. That is, Turkcell was welcome until the IRGC complained*. Turkcell would have been in direct competition with IRGC communications technology and electronics firms. The Council of Guardians—an executive body close to the IRGC and the supreme leader—protested that Iranians would have only 30 percent ownership of the new company. Even after the National Bank of Iran bought out foreign investors to achieve a 51 percent Iranian stake, *the IRGC was not satisfied*. The IRGC-operated [IEI] and the [Bonyad Mostazafan]—an independent financial body *traditionally run by a retired IRGC commander and used by the state as a proxy to fund off-the-books IRGC operations*—erected a

³³⁹ U.S. Treasury Dep't, *Fact Sheet: New Executive Order Targeting Human Rights Abuses Via Information Technology*, (Apr. 23, 2012).

cascade of legal and practical obstacles leading Turkish investors to retreat from the Iranian market.

The IRGC rooted its rhetoric on Turkcell in national security. ... ***the IRGC expects to maintain its dominant position not only on the battlefield, but in civilian sectors as well.*** ... Because some of the Iranian economy's most advanced technological undertakings occur under the aegis of the IRGC and within the framework of the Iranian arms industry, the IRGC can monopolize the transfer and adaptation of high technology to civilian applications ... The homepage of [IEI] ... display[s] many consumer goods produced by the arms industry for sale in the Iranian market. The list includes personal computers, scanners, telephone sets and intercoms, mobile phones, and telephone sim cards. These ***purchases support ... IRGC operations***³⁴⁰

991. As national security analysts Elliot Hen-Tov and Nathan Gonzalez wrote in the *Washington Quarterly* in 2011, Hezbollah, the Qods Force, and Regular IRGC “‘cashed in’ since 2005.”³⁴¹ Describing the “dramatic increase” in the IRGC’s “economic importance” since 2005, they explained that:

[T]he Guards [i.e., the IRGC] controlled less than five percent of GDP shortly after the end of the Iran-Iraq War in 1989. Now, they directly or indirectly oversee ... about 35 percent and growing. ... Prior to 2005, the Guards ... occasionally ***used raw power to reverse high-profile tenders in their favor.*** One of the ***most notable examples*** is when it nullified Turkcell’s winning bid to operate a second mobile-phone network as part of a consortium [in favor of Co-Conspirator MTN]. Upon ***pressure by the Guards*** and their patrons, the Majles was ***forced to change the terms of the deal and revoke Turkcell’s majority share in the consortium.*** After Turkcell’s departure, an Iranian-led consortium ***under the ownership of a Guards’ subsidiary*** [i.e., Co-Conspirator MTN Irancell] received the license for the network.³⁴²

992. Defendants also helped Hezbollah, the Qods Force, and Regular IRGC arm their terrorist proxies al-Qaeda and the Taliban by providing embargoed dual-use technology from the

³⁴⁰ Ali Alfoneh, *How Intertwined Are the Revolutionary Guards in Iran’s Economy?*, American Enterprise Institute, (Oct. 22, 2007) (emphasis added).

³⁴¹ Elliot Hen-Tov and Nathan Gonzalez, *The Militarization of Post-Khomeini Iran: Praetorianism 2.0*, *The Washington Quarterly* (Winter 2011).

³⁴² *Id.* (emphasis added).

United States. Defendants' contribution to the terrorist enterprise was essential, as the embargoed American technology that Defendants provided to the IRGC fronts, including its Hezbollah Division and Qods Force, directly improved the efficacy of the IRGC-supported bombs that the Syndicate used to attack Americans in Afghanistan between 2012 and 2017.

993. The technology Defendants supplied also helped Hezbollah, the Qods Force, and Regular IRGC to logistically support al-Qaeda and Taliban, including Haqqani Network, cells operating in Afghanistan, as well as such group's support cells operating outside of Afghanistan in places like the U.A.E., Pakistan, Iraq, Iran, and other key geographies from which al-Qaeda and the Taliban directly supported the Afghanistan Terror Campaign.

994. As a result of the foregoing, each time Defendants publicly touted how each had helped improve the technical capabilities of the phones and other network devices supplied to MTN Irancell, TCI, or MCI, ZTE and Huawei (alongside co-conspirator MTN) were also admitting that they were bolstering the communications networks, technologies, and operative phones relied upon by Hezbollah, the Qods Force, and Regular IRGC to sponsor al-Qaeda's and the Taliban's terrorist attacks against Americans in Afghanistan.

995. The technology Defendants provided also helped Hezbollah, the Qods Force, and Regular IRGC communicate with Hezbollah and the Qods Force, and IRGC proxies al-Qaeda and the Taliban, in Afghanistan and throughout the Middle East, by sourcing embargoed dual-use technology from the United States. Indeed, the IRGC's desire to ensure that it could securely communicate with its proxies, including al-Qaeda and the Taliban, was what initially motivated it to instruct ZTE and Huawei (alongside co-conspirator MTN) to obtain the embargoed U.S. technology. And for good reason: for a terrorist alliance seeking to evade the surveillance of the world's greatest military so that it could plan its attacks unmolested, sensitive communications

technology from the United States offered an almost impossible-to-overstate communications advantage to the terrorists by arming them with state-of-the-art communications and encryption technology. As the RAND Corporation explained:

For security forces monitoring terrorist communication, such mode nimbleness can *increase the challenges of successfully using terrorist communication traffic*. ... *Terrorist access to easy-to-use devices with multiple modes of communication present challenges for security forces* attempting to intercept or track communications ... Such communication networks can bypass security forces' centralized monitoring at switches or through the intermediate organization that manages the network infrastructure, *and thereby provide fairly secure communication* ...³⁴³

996. Defendants' direct provision of "free goods" to Taliban, including Haqqani Network, terrorists in the form of free cell phones directly facilitated attacks against Americans in Afghanistan. The Taliban's, including its Haqqani Network's, ability to access a river of cell phones from the IRGC, including Hezbollah, and from U.S. and international companies -- both of which channels the ZTE Defendants directly facilitated -- keyed the Taliban fundraising and communications campaigns that formed the foundation of the terrorists' victory in Afghanistan in 2021. After Kabul fell, Tim Culpan, a technology columnist for Bloomberg, explained:

[A] few years after the defeat of the U.S. military in 2001, militant Islamists who had once shunned technology ... coordinated their political and operational messages through a *network of mobile phones*. The decision to incorporate, rather than reject, 21st-century advances became a key factor in the [terrorists'] survival and eventual recovery of [Afghanistan in 2021].

"[The Taliban] moved toward much greater technological sophistication around 2007. It's a sign of the group's ability to adapt and learn, and that's *one of the reasons they won*," said Vanda Felbab-Brown, senior fellow and director of the Brookings Institution's Armed Non-State Actors Initiative. "One of the things they learned was to focus on communications, and to leave behind the model of the 1990s, which was to move the country away from any kind of modernity." ...

By 2007, ... in the midst of the insurgency against the Americans, the Taliban were using monochrome flip phones from brands like Nokia and Motorola to push propaganda and keep tabs on people. Felbab-Brown recalls visiting Afghanistan at the time, when the movement was sending mass, targeted

³⁴³ *Id.* at 35-36 (emphasis added).

text messages. They included reminders to pay *zakat* (religious tax) and that the group knew where he lived.

An irony is that this widespread deployment of telecommunications was made possible by U.S. and international companies Before long, Taliban spokesmen fluent in English were regularly and directly updating Western media by text and voice, answering questions and proclaiming victory in battles journalists didn't even know had happened.

At first, the Taliban were seen by foreign powers, and perhaps even by themselves, as a small, fast military force equipped mainly with rifles and RPGs. But with a more modern enemy like the United States and its allies came the need to add psychological operations. “That's where technology is crucial, there's no way around it,” says Kamran Bokhari, director of analytical development at the Newlines Institute for Strategy & Policy. “Previously they could do without it, but after 9/11 the world changed.”

The Taliban needed to catch up with innovations on the battlefield, and they learned fast. ... And they *weren't just learning from their enemies*. Their fellow jihadists, such as al-Qaeda, ISIS, *and Hezbollah*, had discovered the power of digital technologies to recruit members, threaten opponents, and control messages. The *Taliban benefited from a cross-pollination of the craft* in propaganda and information warfare.

These groups followed the development of technology in the rest of the world. ... [which resulted in] ... the use of more sophisticated handheld devices and faster networks that meant a video could be recorded on a cell phone and e-mailed directly to supporters or international media. The Taliban and their ilk became early adopters ... A key strategy was not only to win battles, but also to shape perceptions of strength and capabilities ... As the US moved into its second decade of occupation, the Taliban kept up a steady drumbeat of messaging across all media, targeting local Afghan forces and governments overseas. The aim was to create the belief that the movement's ascendancy was inevitable and that resistance was futile. The perception helped bring US administrations to the table and may have led to the collapse of the military.³⁴⁴

1. Command, Control, Communications, And Intelligence

997. Command, Control, Communications, and Intelligence (or C3i) are a fundamental cornerstone to all military operations.³⁴⁵ Without C3i, military operations cannot be

³⁴⁴ Tim Culpan, *Technology Fueled the Taliban's Comeback*, NoticiasFinancieras – English (August 23, 2021), 2021 WLNR 27452700

³⁴⁵ Lieutenant Colonel Dale E. Fincke, *Principles of Military Communications for C3i*, Army War College School of Advanced Military Studies, (May 20, 1986), <https://apps.dtic.mil/sti/pdfs/ADA174214.pdf>.

synchronized to effect combat operations at a specific time and place. These principles apply not only to legitimate military operations, but are necessary to effect terrorist operations as well.

998. As General George W. Casey explained in 2009: “Technology is [a] double-edged sword. Inexpensive access to information enables entrepreneurs and innovators to *collaborate in developing new technologies* and improving existing ones. Yet our adversaries can *exploit these same technologies to export terror around the globe*.”³⁴⁶ He continued:

The Israeli-Hezbollah conflict also illustrates the potential impact of hybrid threats. Hezbollah employed modern civil technology (secure cell phones, computers and video telecommunications systems) combined with military means (antitank, surface-to-air and antiship missiles, rockets, mortars and unmanned aerial vehicles) and improvised explosive devices in an innovative array of unanticipated patterns.³⁴⁷

999. Defendants’ sourcing of illicit technologies for Hezbollah, the Qods Force, and Regular IRGC enabled the IRGC to accomplish its Revolution in Terrorist Affairs, to devastating effect.

1000. “In future operational environments,” General Casey warned, “where the tactical environment and strategic environment will often be seamless, it is the network that will provide the ability to gain and maintain the operational advantage.”³⁴⁸ When General Casey wrote this, Hezbollah, the Qods Force, and Regular IRGC was already well on its way to becoming the

³⁴⁶ General George W. Casey, Jr., *The Army of the 21st Century*, Army (Oct. 1, 2009), 2009 WLNR 30869494.

³⁴⁷ *Id.*

³⁴⁸ *Id.*

world's first fully networked terrorist organization, resourced by Defendants' multi-national corporate muscle.³⁴⁹

1001. Indeed, in 2010, General Casey called attention to Hezbollah's use of cell phones and secure computers for command and control, which allowed Hezbollah to inflict far higher casualties on their Israeli enemies: "[Hezbollah] had *secure cell phones, used secure computers for command and control and got their message out* on local television, and about 3,000 Hezbollah operatives basically held off 30,000 well-armed, well-equipped Israeli soldiers."³⁵⁰

1002. **Interoperability.** Defendants also ensured that Hezbollah, the Qods Force, and Regular IRGC realized enormous gains in terrorist effectiveness and lethality based upon the unique interoperability advantages that ZTE Corp. and Huawei Co. (alongside co-conspirator MTN), afforded to the IRGC and its terrorist allies.

1003. **Intelligence.** Defendants also ensured that Hezbollah, the Qods Force, and Regular IRGC achieved a generational improvement in their intelligence collection. As one analyst told the *Christian Science Monitor*, "[m]obile phone networks and how they connect is one of the IRGC's key priorities because it's one of the key tools for opponents," and concluded the IRGC was "improving its connectivity and information-sharing."³⁵¹

³⁴⁹ Indeed, Hezbollah's leader, Hassan Nasrallah, declared that Hezbollah's control of an independent fiber-optic-based cellular network was its "Number One weapon," and compared attacking it to an attack on his person.

Cam Simpson, *Lebanon Deal Boosts Hezbollah; Islamists Gain After Battle Over Secret Fiber-Optic Network*, Wall Street Journal (May 22, 2008) ("[I]t is forbidden to touch [anything] linked to the networks, whether an engineer, a company or a mayor. Touching them is like touching me.").

³⁵⁰ J.D. Leipold, *CSA Addresses Worldwide Challenges at Brookings Institution*, Defense Department Documents (Feb. 2, 2010), 2010 WLNR 2196129.

³⁵¹ Jason Athanasiadis, *How Iranian Dissidents Slip Through Tehran's Airport Dragnet*, Christian Science Monitor (Feb. 8, 2010), 2010 WLNR 2676528.

1004. MTN Group, MTN Dubai, ZTE Corp, and Huawei Co. served as corporate “covers” for Hezbollah, the Qods Force, and Regular IRGC and intentionally structured transactions, supplier relationships, and pricing decisions, among other things, for the specific purpose of illicitly obtaining state-of-the-art American technology, like enterprise level servers. The end goal: transfer the illicitly obtained goods to Hezbollah, the Qods Force, and Regular IRGC for their use in the terrorist campaign against Americans around the world. By serving as corporate “covers” for Hezbollah, the Qods Force, and Regular IRGC each Defendant significantly increased the potency of the scheme, as demonstrated by how long it has endured.

2. Terrorist Finance

i. Cash Flow From MTN Irancell And TCI Revenue

1005. Hezbollah, the Qods Force, and Regular IRGC derived substantial terrorist funding from the billions of dollars in MTN Irancell and TCI-related cash flows, and at least hundreds of millions of dollars annually.

1006. From 2005 through the present, MTN Group’s and MTN Dubai’s illicit transactions with MTN Irancell, the Bonyad Mostazafan, IEI, TCI (including MCI), Exit40, and/or the Akbari Fronts, provided millions, annually, in illicit funds, weapons, and operational support to Hezbollah, the Qods Force, and Regular IRGC, which the IRGC flowed through to its al-Qaeda and the Taliban, including its Haqqani Network, terrorist proxies, who used such resources to attack Americans in Afghanistan, including Plaintiffs and their loved ones.

1007. MTN Group and MTN Dubai significantly increased the cash flowing through MTN Irancell and TCI, and ultimately deployed by Hezbollah, the Qods Force, and Regular IRGC. They did so by illicitly supplying the state-of-the-art American technologies, like servers, to MTN Irancell and TCI, and by extension the IRGC (including Hezbollah and the Qods Force) needed to attack Americans abroad.

1008. By illicitly helping MTN Irancell expand the footprint of its network, MTN Group helped generate new cash flow by connecting more customers to MTN and therefore causing more money to flow through MTN Irancell to Hezbollah, the Qods Force, and Regular IRGC.

1009. As a matter of economic first principles, MTN Group's and MTN Dubai's participation in MTN Irancell caused the latter to become more profitable, because MTN Group was able to bring its networking expertise to the table.

1010. MTN's logic compels this conclusion. According to Gordon Kyomukama, Chief Technical Officer of MTN, "[a]t MTN, extending the footprint of our network and services to *ensure that we connect more people* has been and remains a high priority for our company."³⁵²

1011. On information and belief, on or about 2012, MTN Group began discussions with one or more components of the U.S. government concerning MTN Group's desire to repatriate hundreds of millions of dollars from MTN Irancell.

1012. The financial, technical, communications, intelligence, and operational support that that ZTE Corp. and Huawei Co. (alongside co-conspirator MTN), and their respective U.S. manufacturers provided to their IRGC-controlled, including Qods Force-controlled, counterparties flowed through to al-Qaeda and the Taliban, including its Haqqani Network, through some channels that were "official" and some that were "off-the-books."

1013. From 2003 through the present, Hezbollah, the Qods Force, and Regular IRGC supplied al-Qaeda and the Taliban – directly to each constituent member – with substantial and

³⁵² Intelsat, *Press Release: Uganda Joins Forces with Intelsat, ITSO and MTN to Accelerate 3G Network Infrastructure Deployment in Rural Areas* (May 4, 2018), <https://investors.intelsat.com/news-releases/news-release-details/uganda-joins-forces-intelsat-itso-and-mtn-accelerate-3g-network>.

regular arms deliveries, financial aid, training, logistical support, communications technology (including secure American mobile phones), safe haven assistance, and aid with narcotics trafficking, each form of aid facilitated their shared terrorist enterprise against America (i.e., the conspiracy), which the IRGC's Shiite Terrorist Proxies and IRGC's Syndicate Terrorist Proxies used to aid the terrorists' ability to execute the attacks that injured Plaintiffs.

1014. The embargoed dual-use American technology –included the annual funneling of thousands of secure American smartphones, hundreds of millions of U.S. Dollars, and a vast network of logistical and operational support for the Irancell and TCI fronts that MTN Group, MTN Dubai, ZTE Corporation, and Huawei Corporation provided to their counterparties controlled by Hezbollah, the Qods Force, and Regular IRGC. This technology flowed through to the al-Qaeda and Taliban terrorists who committed each attack that injured each Plaintiff, through transfers made by Hezbollah, the Qods Force, and Regular IRGC to al-Qaeda and the Taliban, including its Haqqani Network.

1015. With respect to MTN Group's, MTN Dubai's, ZTE Corporation's, and Huawei Corporation's "official" transactions with the IRGC, including Hezbollah and Qods Force, front counterparties – which, though notorious, were still illegal – flowed through Hezbollah, the Qods Force, and Regular IRGC into the specific terrorist organizations upon which the IRGC relied to conduct Iranian "security" operations outside of Iran including, but not limited to:

- (i) **Hezbollah's External Security Organization Budget:** In order to fund, arm, train, equip, and logistically support designated terrorist groups, or forward deployed Hezbollah terrorists, that joined the conspiracy to attack Americans including, but not limited to:
 - a. Hezbollah's forward deployed operatives worldwide, including but not limited to, Hezbollah attack planners, bomb makers, logisticians, trainers, attack cells, fundraisers, financiers, propagandists, and videographers, all of whom were regularly forward deployed, under IRGC doctrine, to help commit and plan terrorist attacks alongside local proxy groups (e.g., Jaysh al-Mahdi in Iraq or the Taliban in

- Afghanistan) wherever Americans were found, including, but not limited to, Iraq, Iran, Lebanon, Syria, Yemen, Bahrain, the U.A.E., Afghanistan;
- b. The other Hezbollah terrorists who forward deployed to support Iranian terrorist proxies worldwide, including, but not limited to, al-Qaeda and the Taliban, including its Haqqani Network.
- (ii) **The Qods Force’s “Security” Budget:** In order to fund, arm, train, equip, and logistically support designated terrorist groups that specifically targeted Americans including, but not limited to:
- a. Hezbollah and, through Hezbollah, Jaysh al-Mahdi, including Jaysh al-Mahdi Special Group Asaib Ahl al-Haq, and Jaysh al-Mahdi Special Group Ka’taib Hezbollah, in order to facilitate terrorist attacks against Americans in Iraq and, in the case of Hezbollah, worldwide, including, but not limited to, Iraq, Syria, Yemen, Afghanistan, through cooperation with al-Qaeda and the Taliban including its Haqqani Network, and Europe (collectively, “IRGC Shiite Terrorist Proxies”);
 - b. al-Qaeda, al-Qaeda-in-Iraq, which later became ISIS, Hamas, Palestinian Islamic Jihad, al-Nusra Front, the Taliban, including its Haqqani Network, and Lashkar-e-Taiba, in order to facilitate terrorist attacks against Americans worldwide, including, but not limited to, Iraq, Syria, Yemen, Afghanistan, and Europe through cooperation with al-Qaeda and the Taliban including its Haqqani Network, and Europe (collectively, “IRGC Syndicate Terrorist Proxies”).

1016. The millions in value that ZTE Corp. and Huawei Co. (alongside co-conspirator MTN), and their respective U.S. manufacturers, Defendants ZTE USA, ZTE TX, Huawei USA, Huawei Device USA, and Skycom, each showered upon Hezbollah, the Qods Force, and Regular IRGC each year: For MTN, from 2005 until the present; for ZTE, from at least 2008 through at least 2016; and for Huawei, from at least 2008 through at least 2014. Their official transactions flowed through Hezbollah to the terrorist(s) that committed each attack against each Plaintiff.

1017. MTN Group’s, MTN Dubai’s, ZTE Corp.’s, Huawei Co.’s, and their respective U.S. manufacturers, Defendants ZTE USA, ZTE TX, Huawei USA, Huawei Device USA, and Skycom’s covert “off-the-books” assistance to the terrorists was no less important. Hezbollah, the Qods Force, and Regular IRGC provided tens of millions of dollars “off-the-books” to Hezbollah and (through Hezbollah) to local terrorist proxies since Hezbollah’s inception.

Defendants' "off-the-books" financial-, technology-, and services-related transactions with their IRGC, including Hezbollah Division and Qods Force, front counterparties also flowed through the IRGC, its Hezbollah Division and Qods Force, into Hezbollah's, the Qods Force's – and ultimately their proxies' – terrorist budgets in order to fund the attacks committed by al-Qaeda and the Taliban, including its Haqqani Network, in Afghanistan that injured each Plaintiff. ZTE's and Huawei's (alongside co-conspirator MTN's) illicit transactions with the Bonyad Mostazafan, IEI, MTN Irancell, TCI (including MCI), the Akbari Fronts, and/or Exit40 provided millions in illicit "off-the-books" income, often in U.S. dollars, to Hezbollah, the Qods Force, and Regular IRGC each year, which Hezbollah, the Qods Force, and Regular IRGC then provided to al-Qaeda and the Taliban, including its Haqqani Network so that al-Qaeda and the Taliban could commit each attack that injured each Plaintiff, which they did.

1018. On information and belief, from 2006 through on or about 2010, the IRGC diverted approximately twenty percent (20%) of its net income cash flow from MTN Irancell to the IRGC, Qods Force, and Hezbollah, with each receiving a similar amount each year. At those rates, MTN Irancell caused, at least, more than thirty million dollars to flow through the IRGC to the Qods Force each year, and MTN Irancell caused more than thirty million dollars to flow to Hezbollah each year, and MTN Irancell caused more than thirty million dollars to flow to the IRGC each year. Such cash flows were delivered in regular, predictable amounts, and supported Qods Force and Hezbollah operations, weapons purchases, and personnel costs, among other expenses, in support of anti-American terrorist operations by Qods Force and Hezbollah throughout the Middle East including, but not limited to, Iran, Iraq, Lebanon, Afghanistan, Syria, and Yemen.

1019. On information and belief, after economic sanctions began to hammer the IRGC on or about 2010, the IRGC responded by cutting spending across the board in half, and therefore cut the cash flow through from MTN Irancell to the IRGC, Qods Force, and Hezbollah from twenty percent (20%) to ten percent (10%), with each receiving a similar amount each year. At those rates, MTN Irancell caused, at least, more than fifteen million dollars to flow through the IRGC to the Qods Force each year, and MTN Irancell caused more than fifteen million dollars to flow to Hezbollah each year. Such cash flows were delivered in regular, predictable amounts, and supported Qods Force and Hezbollah operations, weapons purchases, and personnel costs, among other expenses, in support of anti-American terrorist operations by Qods Force and Hezbollah throughout the Middle East including, but not limited to, Iran, Iraq, Lebanon, Afghanistan, Syria, and Yemen.

**ii. Cash Flow From Terrorist Fundraising Campaigns,
Procurement Bribery, Khums, And Financial Management**

1020. Defendants' assistance facilitated terrorist fundraising campaigns by Hezbollah, the Qods Force, and Regular IRGC that directly supported attacks in Afghanistan and Iraq by channeling resources to the IRGC and its terrorist allies.

1021. Defendants' procurement bribes facilitated terrorist fundraising campaigns by Hezbollah, the Qods Force, and Regular IRGC that directly supported attacks in Afghanistan and Iraq by channeling resources to the IRGC and its terrorist allies.

1022. Defendants' indirect donations (*khums*), meaning the cash flow that Defendants triggered when they paid Hezbollah, the Qods Force, and Regular IRGC (e.g., when they bribed an IRGC cutout in Dubai), facilitated terrorist fundraising campaigns by Hezbollah, the Qods Force, and Regular IRGC that directly supported attacks in Afghanistan and Iraq by channeling resources to the IRGC and its terrorist allies.

1023. Defendants assisted Hezbollah, the Qods Force, and Regular IRGC to revolutionize their financial management capabilities, which meant that the terrorists had more resources upon which to draw for killing Americans.

3. Weapons

i. Improvised Explosive Devices (IEDs)

1024. ZTE and Huawei (alongside co-conspirator MTN) also supported the terrorist campaign through their financial support of fronts acting for Hezbollah, the Qods Force, and Regular IRGC which provided them funds, bomb parts, and other necessary material vital to al-Qaeda's and the Taliban's, including its Haqqani Network's, ability to conduct a nationwide IED campaign targeting Americans in Afghanistan. Hezbollah, the Qods Force, and Regular IRGC manufactured and/or sourced key components for the Syndicate's IED attacks, including, but not limited to, the military- and factory-grade embargoed communications technologies, which al-Qaeda and the Taliban, including its Haqqani Network, used and were vital to the Syndicate's ability to build the advanced al-Qaeda-designed CAN fertilizer bombs (IEDs and suicide bombs) that benefited from the upgraded communications technologies provided by the IRGC, which helped al-Qaeda and the Taliban defeat the American countermeasures designed to protect Plaintiffs from al-Qaeda's bomb attacks, and which al-Qaeda and the Taliban used to commit many of the IED attacks that injured Plaintiffs.

1025. ZTE's and Huawei's (alongside co-conspirator MTN's) conduct had an especially tight nexus with al-Qaeda's and the Taliban's, including its Haqqani Network's, ability to execute signature al-Qaeda attacks involving the use of CAN fertilizer bombs, advanced rockets, and hostage-taking. Each IED and advanced rocket that al-Qaeda and the Taliban used to attack and injure each Plaintiff contained, reflected, was reverse-engineered from, and/or was otherwise technologically aided by Hezbollah's, the Qods Force's, and Regular IRGC's use of embargoed

American technology. In the case of Huawei, that embargoed American technology was obtained by and through, on information and belief, Huawei's subsidiaries and employees in the U.S., including but not limited to Huawei USA, Huawei Device USA, and Futurewei. In the case of ZTE, that embargoed American technology was obtained by and through, on information and belief, ZTE's subsidiaries and employees in the U.S., including but not limited to ZTE USA and ZTE TX. In the case of MTN, MTN provided such technology pursuant to MTN Group Limited's joint venture with Hezbollah, the Qods Force, and Regular IRGC through MTN Irancell. The embargoed American technology that MTN, ZTE (via ZTE USA and ZTE TX), and Huawei (via Huawei USA, Huawei Device USA, and Futurewei) covertly supplied to Hezbollah, the Qods Force, and Regular IRGC substantially improved the efficacy and lethality of each EFP and rocket used to attack and injure each Plaintiff.

1026. ZTE and Huawei (alongside co-conspirator MTN) also supported the terrorist campaign through their financial support of fronts acting for Hezbollah, the Qods Force, and Regular IRGC, which funded al-Qaeda's and the Taliban's, including its Haqqani Network's, attacks against Americans in Afghanistan. Hezbollah, the Qods Force, and Regular IRGC manufactured and/or sourced key components for the Syndicate's IED, rocket, and kidnapping attacks, including, but not limited to, the military- and factory-grade embargoed communications technologies, which al-Qaeda and the Taliban used and were vital to al-Qaeda's and the Taliban's ability to build the advanced al-Qaeda-designed IEDs that al-Qaeda and the Taliban used to commit many IED attacks that injured Plaintiffs.

ii. Rockets

1027. Defendants' assistance directly improved the lethality and accuracy of the rockets deployed by Hezbollah, the Qods Force, and Regular IRGC.

4. Recruiting, Fundraising, Strategic Communications, And Disinformation

1028. The IRGC, including its Hezbollah Division and the Qods Force, emphasized the centrality of orchestrated propaganda campaigns to drive recruiting and fundraising, strategic communications to deliver custom messages to custom audiences, and broad disinformation campaigns to conceal the conspiracy. The terrorists devoted so much time to these efforts for an obvious reason: they played a vital role in furthering the conspiracy and maximizing the number of Americans the terrorists could kill in Afghanistan, Iraq, and throughout the Middle East. “Based on their extensive reach in the communications economy,” according to Ms. Gill, “the IRGC orchestrated a ‘comprehensive messaging strategy’ using radio and television broadcasts, newspapers, websites, and social media accounts to amplify the message that the Islamic Republic was under attack from the West. Using media infrastructure ... and telecommunications infrastructure ..., the IRGC actively engaged the communications economy in defending the Islamic Republic against the soft war tactics of the West.”³⁵³

1029. In so doing, the conspiracy leveraged the explosion of information technologies and computing power since 2000. As the United Nations Office on Drugs and Crime (“UNODC”) documented in 2012:

Technology is one of the strategic factors driving the increasing use of the Internet by terrorist organizations and their supporters for a wide range of purposes, including recruitment, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes. While the many benefits of the Internet are self-evident, it may also be used to facilitate communication within terrorist organizations and to transmit information on, as well as material support for, planned acts of terrorism,

³⁵³ Gill, *Capitalism, Communications, and the Corps*, at 110.

all of which require specific technical knowledge for the effective investigation of these offences.³⁵⁴

i. Recruiting and Fundraising

1030. Islamist terrorists have widely relied upon antisemitic appeals to raise money, recruit followers, and gain other advantages. The Anti-Defamation League observed in 2015:

Fourteen years after 9/11, terrorist groups motivated by Islamic extremist ideology, from Al Qaeda to the Islamic State of Iraq and Syria (ISIS), continue to rely on depictions of a Jewish enemy – often combined with violent opposition to the State of Israel – to recruit followers, motivate adherents and draw attention to their cause. Anti-Israel sentiment is not the same as anti-Semitism. However, terrorist groups often link the two, exploiting hatred of Israel to further encourage attacks against Jews worldwide and as an additional means of diverting attention to their cause.³⁵⁵

1031. Few terrorists are more committed to this strategy than Hezbollah, the Qods Force, and Regular IRGC who have long used baldly antisemitic propaganda as a core part of their terrorist conspiracy, by spreading the hateful slur that the United States and Israel are part of a Jewish-led cabal seeking to take over Muslim lands.

1032. The IRGC's campaign to spread hateful antisemitic propaganda about Israel, the United States, and people of the Jewish faith were not the idle musings of disorganized radical Islamists blogging out of their parents' basements. These were industrial scale, IRGC- and Hezbollah-administered propaganda campaigns that sought to strengthen the terrorist conspirators' ability to attack Americans worldwide by, among other things: (1) **bolster terrorist fundraising** by increasing the potency of the terrorists' online fundraising appeals, and

³⁵⁴ United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* at 1 (Sept. 2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

³⁵⁵ Anti-Defamation League, *Anti-Semitism: A Pillar of Islamic Extremist Ideology* at 1 (2015), <https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/Anti-Semitism-A-Pillar-of-Islamic-Extremist-Ideology.pdf>.

thereby drive more dollars to the terrorist campaign; (2) **recruit more terrorists** by creating the initial touchpoints for new recruits, e.g., a 16-year old watches a splashy Hezbollah video and decides to join the group; and (3) **enhance the terrorists' concealment** by flooding the zone with propaganda designed to persuade the population to support the terrorists or, at least, not rat them out to the Americans nearby (almost as good), by portraying a common enemy.

1033. Regular media discussions also specifically alerted Defendants that the IRGC, including its Hezbollah Division and the Qods Force deployed antisemitic propaganda to raise money and recruit terrorists.

1034. In furtherance of the conspiracy, MTN Group and MTN Dubai were, and remain to this day, one in spirit with the antisemitic terrorist recruiting messaging of the IRGC, including Hezbollah, and the Qods Force, as well as their co-conspirators in Syria (like the Assad regime) and Afghanistan (like al-Qaeda and the Taliban, including its Haqqani Network).

1035. *First*, MTN Group and MTN Dubai regularly enabled the creation, uploading, distribution, downloading, and propagation of a near-constant 24/7 river of terrorist recruitment appeals by, among others, the IRGC, Hezbollah, and the Qods Force, through their provision of technical, financial, operational, and personnel support to MTN Irancell and MTN Syria, both of which reinforced the recruiting campaigns.

1036. *Second*, MTN Group and MTN Dubai have never publicly condemned the antisemitic terrorist propaganda they have enabled in Iran (through MTN Irancell), Syria (through MTN Syria), Yemen (through MTN Yemen), and Afghanistan (through MTN Afghanistan). In every country, MTN Group and MTN Dubai facilitated the local MTN subsidiary's direct and indirect assistance to the recruiting campaigns, all of which followed the

Hezbollah playbook of using over-the-top bile to raise awareness for recruiting drives, fundraising solicitations, and more.

1037. MTN Group and MTN Dubai were (and remain) one in spirit with the IRGC's, including Hezbollah's and the Qods Force's, antisemitic terrorist recruiting message. Most obviously, MTN Group and MTN Dubai are the but-for cause of the terrorists' ability to spread their recruitment pitches so effectively through the litany of terrorist-enabling services that MTN Group committed every MTN subsidiary and affiliate to provide to all "Iranian Shareholders," i.e., the IRGC, including its Hezbollah Division and the Qods Force, which substantially bolstered the terrorists' antisemitic recruiting and fundraising pitches.

1038. Since 2005, MTN Group and MTN Dubai have broadcast the terrorists' antisemitic recruiting propaganda throughout the Middle East while never once publicly stating that: (a) Israel has a right to exist; (b) bomb attacks against Americans in the Middle East by Iranian proxies are wrongful; or (c) the Holocaust should be remembered. The reason is obvious—MTN agrees with its terrorist business partner: they are one in spirit.³⁵⁶

ii. Strategic Communications and Disinformation

1039. After 9/11, Hezbollah, the Qods Force, and Regular IRGC was keenly aware how an effective strategic communications (or "stratcoms") campaign could directly aid their transnational terrorist conspiracy. Indeed, no major global terrorist organization has a longer,

³⁵⁶ A Westlaw News search designed to obtain any media report containing the phrases "MTN Group" or "MTN Dubai" within 100 words of the roots for Israel and antisemitism (Westlaw News "MTN Group" or "MTN Dubai" /100 Israel! Antisem! Holocaust!) reveals approximately 300 documents as responsive hits. Nothing. A comprehensive Google search similarly reveals no statement. MTN Group could, of course, cease broadcasting terrorist propaganda, publicly issue a sweeping defense of Israel's right to exist, and unequivocally condemn roadside bomb attacks supported by Iran. MTN Group's obvious refusal to do so in nearly two decades flies so contrary to international corporate norms, only one conclusion results: MTN Group and the IRGC are one in spirit.

more prolific, or more impactful record of turning effective strategic communications campaigns into new sources of funds, personnel, safehouse, and the litany of other functions that required an ever-growing group of allies and enablers.

1040. The U.S. military concluded long ago that there was a direct relationship between effective strategic communications and overall probability of success on a given venture. This reflects a recognition, as General George W. Casey, Jr., explained, “Conflicts” will continue to take place under the unblinking scrutiny of the 24-hour media cycle and the World Wide Web.... Adversaries will have many forums in which to disseminate their messages worldwide.”³⁵⁷

1041. Hezbollah, the Qods Force, and Regular IRGC also understood that effective strategic communications were necessary to further the conspiracy by, among other things, promoting a disinformation campaign designed to conceal the conspiracy by causing the spread of falsehoods relating to it, and preventing controversies that could expose co-conspirators, incentivize people to exit the conspiracy, or foreseeably cause a co-conspirator to be financially or logistically unable to continue supporting the conspiracy, such as a threat that could cause a corporate co-conspirator to lose billions of dollars or cause an individual co-conspirator to lose their life or freedom.

1042. Writing in an official NATO journal in 2020, Ms. Gill explained, “The Invisible Hand of the IRGC” touched every transaction relating to MTN Irancell, TCI, and their associated IRGC front company shareholders and, as a result, “the reliance of the IRGC’s strategic narrative on the communications economy concerns more than explicitly ideological motivations; a

³⁵⁷ General George W. Casey, Jr., *The Army of the 21st Century*, Army (Oct. 1, 2009), 2009 WLNR 30869494.

distinctly coercive element can also be identified. Beyond their devotion to the Construction Jihad, the Guard relied on the communications economy as a tool of power projection.”³⁵⁸

1043. MTN Group coordinated the strategic communications and crisis prevention efforts relevant to the entire terrorist conspiracy, and managed MTN Irancell-related strategic communications and public branding outside of Iran.

1044. Ever since MTN Group committed itself and every MTN subsidiary and affiliate to the conspiracy on September 18, 2005, MTN Group pursued an aggressive, more than decade-long, strategic communications campaign to further the conspiracy.

1045. MTN Group successfully suppressed any leaks, materially negative press reporting, or public sector investigations in the United States, Europe, Africa, or Southeast Asia concerning MTN Group’s and MTN Dubai’s secret agreement with Hezbollah, the Qods Force, and Regular IRGC until on or about March 28, 2012, when Turkcell sued MTN in federal district court in Washington, D.C., at which time a whistleblower revealed the secret Agreement to the world through Turkcell’s lawsuit. On information and belief, MTN Group relied upon effective strategic communications and crisis prevention services to prevent negative information from “leaking” for nearly seven years after the Agreement was signed.

1046. MTN Group’s successful communications strategy prevented any major media scandals concerning MTN Group from between 2005 and 2010. Ordinarily, of course, a parent company’s brand equity is of no moment in an Anti-Terrorism Act case. But when that parent company is, effectively, the joint venture partner of terrorists, as is the case here, and when the

³⁵⁸ Gill, *Capitalism, Communications, and the Corps*, at 108. Ms. Gill concluded that “[w]hilst strategic narratives construct the truth, communications economies enable control over communicative processes; both reinforce one another to create a hegemonic understanding of reality that supports a political actor’s values, interests, or objectives.” *Id.* at 113.

point of the joint venture is to generate cash flow and serve as cover for sourcing illicit weapons parts, then the parent company's brand and reputation are essential.

1047. Simply put, MTN Group began serving as the IRGC's telecommunications- and computing-related financial and logistics agent worldwide in 2005, never stopped doing so, and continues to play the same role today even after the IRGC was designated an FTO. To accomplish that task, MTN Group coordinated a strategy with MTN Dubai to engage in a series of illegal and fraudulent transactions designed to raise money and source key terrorist components from the United States.

1048. When MTN Group and MTN Dubai operated a worldwide campaign to, among other things, illicitly source more than ten thousand (10,000) high-tech American-manufactured smartphones from sellers within the United States to MTN Group and MTN Dubai's crooked agents, employees, and cut-outs worldwide, ***MTN Group and MTN Dubai were acting as a front for Hezbollah and the Qods Force.***

1049. MTN Group's and MTN Dubai's continued service as a terrorist front even after these issues surfaced in litigation in 2012, 2019, and in the instant case. MTN Group and MTN Dubai continue to act as a now notorious front for the IRGC (an FTO), the Qods Force (an FTO), Hezbollah (an FTO), all of whom, as constituent members of the IRGC were, and remain, parties to the Agreement between "MTN" (i.e., all MTN entities worldwide) and the Iranian Shareholders (i.e., all component parts of the IRGC, necessarily including the IRGC's Hezbollah Division and Qods Force). Plainly, they mean to serve as a terrorist front.

1050. In their capacity as long-standing joint venture allies, fundraising partners, and illicit sourcing fronts since 2005, MTN Group and MTN Dubai knew, or were generally aware, that there was a direct, linear, and measurable relationship between MTN Group's and MTN

Dubai's public reputation and brand health on the one hand, and the volume of money and illicitly sourced technology that ultimately flowed through to the IRGC, Hezbollah, the Qods Force, and their terrorist proxies worldwide on the other. On information and belief, such knowledge, or general awareness, extended to, among others: (1) MTN Group's President and CEO; (2) MTN Group's Commercial Director; (3) MTN Group's Board of Directors; (4) MTN Group's in-house counsel and "compliance"³⁵⁹ staff; (5) MTN Group's external advisors; and (6) MTN Dubai's country manager.

1051. The better MTN Group's and MTN Dubai's public reputation and brand health, the more cash to flow through MTN Irancell to the terrorists because, among other reasons: (1) the better MTN Group's and MTN Dubai's brand, the better the sales for MTN Group's joint venture partner, the IRGC, through Irancell; and (2) the easier it was for MTN Group and MTN Dubai to illicitly source the technology demanded by Hezbollah and the Qods Force – especially for the higher-cost items like servers, or unusually large bulk orders of less expensive (but still costly) items, like smartphones. Often, such transactions required that MTN Group, MTN Dubai, and the agents and cut-outs acting on their behalf, transact with suppliers who were more concerned about reputational risk in comparison to the more traditional high-tech black-market resellers for things like smartphones.

1052. From 2005 through at least 2011, MTN Group and MTN Dubai pursued a successful strategic communications campaign that prevented any catastrophic public relations

³⁵⁹ MTN Group and MTN Dubai are actively, and defiantly, aiding multiple Foreign Terrorist Organizations through the ongoing river of cash they are effectively causing to flow to the IRGC, including its Lebanese Hezbollah division and Qods Force, through MTN Irancell, which MTN Group and MTN Dubai refuse to immediately compel to wind down. As such, one may reasonably assume that "compliance" as currently practiced at MTN Group and MTN Dubai is just another euphemism at MTN Group.

scandals in the United States, Europe, Africa, or Southeast Asia concerning MTN Irancell, MTN Group, or any other MTN subsidiary or affiliate that could have undermined MTN Group's and MTN Dubai's ability to serve as "cover" most effectively for the conspiracy's continuing efforts to illicitly source weapons and funds to enable terrorist attacks against Americans globally.

1053. On or about December 2010 or January 2011, MTN Group caused MTN Nigeria to hire Individual 1, a former high-level official in the Obama Administration, ostensibly to give two speeches, for which Individual 1 accepted a \$100,000 speaking fee. On information and belief, MTN Group either wired the \$100,000 to Individual 1's bank account in the United States itself, or MTN Nigeria wired the \$100,000 to Individual 1's bank account at the direction of MTN Group, which thereafter reimbursed MTN Nigeria.

1054. When MTN Group caused MTN Nigeria to pay Individual 1's \$100,000 speaker fee, it was not because MTN Group or MTN Nigeria were interested in Individual 1's speech. Instead, on information and belief, MTN Group caused MTN Nigeria to pay Individual 1, because MTN Group knew that Individual 1 would return to the Obama Administration, and MTN Group intended to induce Individual 1's service as a backdoor communications channel with the White House.

1055. MTN Group paid Individual 1 because MTN Group knew Individual 1 would be immensely influential within the Obama Administration while it was analyzing, among other things, the geopolitical and public messaging concerns attendant to question of whether to soften the then-existing sanctions, which were crushing the IRGC, and therefore undermining MTN Group's joint venture partner – and, by extension, MTN Group.

1056. MTN Group's retention of Individual 1 in December 2010 and indirect payment (through its captive subsidiary, MTN Nigeria) of \$100,000 to Individual 1 was an act in

furtherance of the conspiracy. On information and belief, MTN Group wired \$100,000 to Individual 1, causing it to be received by Individual 1 inside the United States, hoping that Individual 1 would, in effect, be on MTN Group's "side" (or at least, willing to take a meeting) when the time was right concerning the sanctions on MTN Group's JV partner, the IRGC.³⁶⁰

B. Defendants Knew That Their Provision Of "Security" "Cooperation" Aid To Hezbollah, The Qods Force, And Regular IRGC Supported Terrorist Attacks Against Americans In Afghanistan By IRGC Proxies Al-Qaeda And The Taliban Because Defendants Knew That "Security" Was An IRGC Euphemism For The IRGC Proxy Attacks Against Americans

1057. By 2005, Defendants' experiences, communications, and awareness of basic facts concerning Iran alerted Defendants to the fact that Iran's "security" was controlled by the IRGC, Hezbollah, and the Qods Force and such "security" was a widely known euphemism for kidnapping and terrorist attacks against Americans by these groups. Defendants knew that their assistance to Hezbollah, the Qods Force, and Regular IRGC furthered the IRGC's support for terrorists and proxies like al-Qaeda and the Taliban, and constituted an agreement to aid anti-American terrorists that was illegal under U.S. law.

1. In-Person IRGC Communications as Terrorist Tradecraft

1058. Under standard principles of IRGC terrorist tradecraft, each of the "Iranian Shareholders," including but not limited to each Defendants' handlers and contacts at the IRGC, including its Hezbollah Division and the Qods Force, communicated to Defendants the core price of doing business with Irancell and TCI: that they would have to aid the "security" agenda of

³⁶⁰ Plaintiffs have no reason to believe this scheme worked. The effectiveness of MTN Group's transparent attempt to grease a senior insider is not the point. What matters is that MTN Group – more than five (5) years after joining the conspiracy in 2005 – was still coordinating substantial expenditures of time and money for the obvious purpose of improving the economic climate in which MTN Irancell, and by extension the IRGC, operated, and regularly reaching into the United States to do so.

Iran, and in particular, Iran’s transnational terrorist logistics enterprise. MTN Group and MTN Dubai’s experience negotiating with the IRGC from 2004 through 2005 proves it, and the IRGC, on information and belief consistently followed the same approach with ZTE and Huawei. As a result, MTN Group, MTN Dubai, ZTE, and Huawei knew the deal.

2. Iranian Constitution

1059. Defendants knew that Iran’s constitution³⁶¹ distinguishes “security” from other Iranian governmental functions consistent with what Defendants knew — that “security” in Iran means “terror” against Americans outside of it. Examples drawn from Iran’s constitution include, but are not limited to:

Preamble: “[T]he Islamic Revolutionary Guards Corps are to be ... responsible ...for fulfilling the *ideological mission of jihad* in God’s way; that is, *extending the sovereignty of God’s law throughout the world* (this is in accordance with the Qur’anic verse ‘Prepare against them whatever force you are able to muster, and strings of horses, striking fear into the enemy of God and your enemy, and others besides them’ [8:60]).”³⁶²

- (i) Article 145: “No foreigner will be accepted into the Army *or security forces* of the country.”
- (ii) Article 172: “Military courts will be established by law to investigate crimes committed in connection with military *or security duties* by members of the Army, the Gendarmerie, the police, and the Islamic Revolution Guards Corps.”

3. Iranian National Security Council

1060. The Iranian National Security Council’s structure ensured Defendants knew that “security” was a euphemism for Iran-backed terrorist campaigns against the United States worldwide. Most obviously, Iran’s National Security Council is responsible for its terrorist

³⁶¹ https://www.constituteproject.org/constitution/Iran_1989.pdf?lang=en.

³⁶² The emphasized passages are widely understood, inside Iran and around the world, to refer to the IRGC’s foundational mission of attacking the United States around the world in order to advance the Iranian Islamic revolution.

agenda, including Iran’s routine deployment of proxies like Hezbollah to coordinate attack campaigns against Americans globally.³⁶³

4. Hezbollah Structure

1061. Hezbollah’s organizational chart also confirmed that Defendants knew that “security” was a euphemism for terror. As the “Hezbollah Division” of the IRGC, Hezbollah is a subordinate branch of the IRGC, and therefore because the IRGC is in charge of “security” in Iran, it necessarily follows that “security” matters in Iran also include Hezbollah and the Qods Force. Moreover, from the 1990s through the present, the structure of Hezbollah’s purported “terrorist wing”³⁶⁴ has always been officially and publicly referred to as Hezbollah’s “External *Security* Organization.”

5. IRGC Doctrine

1062. Unlike nearly every other terrorist group, the IRGC was founded and explicitly committed to anti-American terror as a matter of Iranian national security doctrine targeting the United States (the “Great Satan”) for external terrorist attacks in order to advance Iran’s Islamic revolution globally. As Dr. Mark Silinsky, a 36-year veteran military intelligence analyst of the U.S. Department of Defense and an affiliated professor at the University of Haifa, explained in 2019:

The third *major goal* of the IRGC is *combatting Iran’s declared enemies, the most reviled of whom are the United States*, Israel, and Saudi Arabia. A leading

³⁶³ See, e.g., Ali Reza Nader (Senior International Policy Analyst at RAND Corp.), *Iran Vote is Cause for Optimism*, Realism, Star Tribune (June 19, 2013) (“A 20-year parliamentarian, Rowhani formerly led *Iran’s security council*, so he has had direct knowledge and/or involvement in Iran’s internal repression and *external support of terrorist organizations like Hezbollah*.”), 2013 WLNR 15146323.

³⁶⁴ Like its IRGC overlords, and Iranian terror proxies like Jaysh al-Mahdi, Lebanese Hezbollah maintains a fictional separation between their “terrorist” and “political” wings, but this is just terrorist tradecraft designed to provide concealment for Hezbollah operatives, and there is no meaningful firewall between the two wings.

IRGC-controlled media outlet claims that those three countries “finance terrorists and provide them with weapons.” Iranian hatred of the United States is deep and enduring. Early in his adulthood, Khomeini named the United States the “Great Satan,” a moniker that endures today. ... Iranian leaders often clamor that the United States has dominated weaker countries for centuries and proclaim that the United States intends to destroy Islam and the Islamic Republic of Iran. In Iran, there are broadcasts, television shows, movies, songs, and video games with the theme of destroying America.³⁶⁵

6. Iran-Focused Scholars

1063. According to a broad consensus of Iran scholars, “security” ordinarily is understood in the Iranian context, by all sides, to refer to IRGC-related terror operations against Americans carried out by the Hezbollah, the Qods Force, and associated terrorist proxies, including, but not limited to:

- (i) Tony Badran, September 2011: “[T]he Qataris also ran their initiative by Tehran, in order to ... assure the Iranians that Syria’s *‘security doctrine’* meaning its policy of *support for so-called ‘resistance movements’ sponsored by Iran* would remain intact.”³⁶⁶
- (ii) Ambassador R. Nicholas Burns, January 2016: “[T]he people who *actually run Iran’s security policies*, their intelligence networks, their *support to the terrorist groups like Hezbollah and Hamas, are in the Iranian Revolutionary Guard Corps*. That group of people has a *fundamentally more anti-American*, cynical, brutal view of the future of Middle East politics.”³⁶⁷
- (iii) Nakhleh Emile, June 2017: “Iran has supported Sunni and Shia terrorist organizations over the years ... in the service of its national interest. *Supporting proxy terrorist groups*

³⁶⁵ Dr. Mark Silinsky, *Iran’s Islamic Revolutionary Guard Corps: Its Foreign Policy and Foreign Legion*, Marine Corps University, Expeditions with MCUP (Digital Journal) (Jan. 2019) (emphasis added), <https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/Irans-Islamic-Revolutionary-Guard-Corps/>.

³⁶⁶ Tony Badran (Research Fellow Foundation for Defense of Democracies), *U.S. Human Rights Policy in Iran and Syria*, Congressional Testimony via FDCH (Sept. 22, 2011) (emphasis added), 2011 WLNR 24786203. Syria and Iran share a common “security doctrine,” which is dictated by the IRGC, including Lebanese Hezbollah and the Qods Force.

³⁶⁷ R. Nicholas Burns, *quoted in interview with Ashish Kumar Sen* (Atlantic Council), *Dealing with Iran: A Policy of Engagement and Deterrence*, Harvard Belfer Center for Sci. & Int’l Affairs, States News Service, (Jan. 19, 2016), (emphasis added).

has been a principle of Iran's security doctrine for years, especially during the period when Iran was threatened with the possibility of regime change.”³⁶⁸

- (iv) Dr. Ronen Bergman and Dr. Raz Zimmt, July 2018: “While the Iranian nuclear program isn’t under the *IRGC’s command*, its *security definitely is*.”³⁶⁹
- (v) Seth Frantzman, July 2020: “Iran said it hoped Iraq would play a greater role in *regional security, apparently meaning* helping Iran work with Syria and perhaps be a conduit for Iran’s weapons trafficking to Syria. Iran has sent ballistic missiles to Iraq in 2018 and 2019 and trafficking precision guided munitions via Iraq’s Al-Qaim border area with Syria. Iraq has recently tried to replace some units on the border to make the border more secure. *Regional security, for Iran, means regional Iranian hegemony*. Iraq is Iran’s ‘near abroad’ in this equation. The pressure on Kadhimi was intense during the recent visit and *Iran showed it means business in terms of pressuring the US to leave Iraq*.”³⁷⁰
- (vi) Ariane Tabatabai, November 2020: “[Qassem] Soleimani and [Mohsen] Fakhrizadeh,” the “head of research and innovation at Iran’s Ministry of Defense,” “were the architects of *two pillars of Iran’s security policy*: its *proxy* and nuclear programs ... Both helped *create the infrastructure* and develop the programs. But their deaths won’t lead to a fundamental change, as institutions will continue the projects.”³⁷¹

7. Terrorist Statements

1064. Public statements by the IRGC, Hezbollah, and the Qods Force also alerted Defendants that “security” was a code word for anti-American terror operations by the IRGC, Hezbollah, and the Qods Force, including, but not limited to:

- (i) BBC, July 2013: “Iran’s MP on *security* and foreign affairs denounce[d] an EU decision to include Hezbollah military wing in the list of terrorist organizations.”³⁷²

³⁶⁸ Nakhleh Emile, *Aligning With Iran Necessary to Combat Sunni Extremism*, Iran Times International (June 9, 2017) (emphasis added), 2017 WLNR 23277897.

³⁶⁹ Dr. Ronen Bergman and Dr. Raz Zimmt, *Israel’s Most Dangerous Enemy: Who Are You, Hajj, Qasem Soleimani?*, Yedioth Ahronoth (Israel) (July 3, 2018) (emphasis added), 2018 WLNR 20323696.

³⁷⁰ Seth J. Frantzman, *Iran’s Maximum Pressure on Iraq to Remove US Forces*, Jpost.com (Jerusalem Post online) (July 22, 2020) (emphasis added), 2020 WLNR 20379547.

³⁷¹ *Quoted in Arkansas Democrat Gazette, Iran Claims Israel, U.S. Linked To Slaying Of Key Nuclear Scientist* (Nov. 28, 2020) (emphasis added), 2020 WLNR 34141033.

³⁷² BBC International Reports (Central Asia), *Programme Summary of Iranian Gorgan Radio News 1600 gmt 24 Jul 13* (July 25, 2013) (emphasis added).

- (ii) Fars News Agency (Iran), February 2014: “An Iranian deputy foreign minister blasted Washington for raising baseless allegations against Tehran, and said the US which supports terrorist groups with financial, political and arms aids cannot accuse others of advocating terrorism. ... ***‘The Lebanese Hezbollah is strongly fighting terrorism in support of the country’s security and stability,’*** the Iranian official added.”³⁷³
- (iii) IRIB World Service (Iran), March 2016: “Iran says a decision by Persian Gulf Arab states to brand Lebanon’s Hezbollah as a terrorist group is a ‘new mistake’ that will undermine peace in the region and unity in Lebanon. ... ***‘Those who call Hezbollah terrorists,*** have intentionally or unintentionally targeted the unity and ***security*** of Lebanon,” Iran’s Deputy Foreign Minister Hossein Amir-Abdollahian said.”³⁷⁴
- (iv) Naharnet (Lebanon), March 2016: “A top Iranian security official ... hailed ... ‘Hizbullah has played a key role in ... protecting Lebanon’s ***security,***’ said Ali Shamkhani, the head of the Supreme National Security Council of Iran.”³⁷⁵
- (v) Seth Frantzman, July 2020: “The Ayatollah stressed that while Iran does not interfere in Iraq, it is the ‘corrupt’ Americans who are interfering in Iraq and who only sow destruction in the region. ... [Iraqi Prime Minister] Kadhimi also met with Ali Shamkhani, the head of the Supreme National ***Security*** Council. Shamkhani has visited Iraq earlier this year to ***pressure Iraq to expel US forces.*** ... Shamkhani’s meeting with Kadhimi was meant to be yet another piece of Iran’s ***maximum pressure to get US forces out of Iraq. Shamkhani said the Us was ‘evil’ and that it was a ‘malicious, terrorist’ element in Iraq that was leading to insecurity.***”³⁷⁶

8. Iran-Related “Security” Media Coverage

1065. Regular media discussions also specifically alerted Defendants that “security” was a code word for anti-American terror operations by the IRGC, Hezbollah, and the Qods Force, including, but not limited to:

³⁷³ Fars News Agency (Iran), *Iran Raps US Double-Standard Policy Towards Terrorism* (Feb. 12, 2014) (emphasis added).

³⁷⁴ IRIB World Service (Iran), *[P]GCC Branding of Hezbollah as Terrorist a New Mistake: Iran* (Mar. 3, 2016), (emphasis added), 2016 WLNR 6748676.

³⁷⁵ Naharnet (Lebanon), *Iran: Hizbullah Played Key Role in Eradicating Terror in Syria, Protecting Lebanon* (Mar. 17, 2016), (emphasis added), 2016 WLNR 8288436.

³⁷⁶ Seth J. Frantzman, *Iran’s Maximum Pressure on Iraq to Remove US Forces*, Jpost.com (Jerusalem Post online) (July 22, 2020), (emphasis added), 2020 WLNR 20379547.

- (i) Denver Rocky Mountain News, April 1992: “Imad Mughniyeh, **chief of security** for Hezbollah, the Iranian-sponsored Party of God, and **head of its terrorist arm**, Islamic Jihad (Holy War).”³⁷⁷
- (ii) San Francisco Chronicle, September 2001: “Arranges security for meeting between bin Laden and Imad **Mughniyeh, security chief for the Iran-sponsored terrorist group Hezbollah**.”³⁷⁸
- (iii) Washington Post, November 2001: “Iran’s foreign and **security policies** ... back terrorist groups such as Hezbollah and Hamas ... Ayatollah Mahmoud Hashemi Shahroudi, the head of Iran’s judiciary, recently summed up the view of this wing of the government: **‘Our national interests lie with antagonizing the Great Satan,’** he stated. ... It would be a mistake for the Bush administration to warm relations without serious progress in reining in Iran’s ... terrorist links.”³⁷⁹
- (iv) Jerusalem Post, June 2002: “Once in southern Lebanon, the 1992 Palestinian deportees, like Jenin Islamic Jihad leader Sheikh Bessam Sa’adi learned **bomb-making and terror techniques** from Hizbullah militants and **Iranian security agents**.”³⁸⁰
- (v) Boston Herald, March 2004: “All this would be news for Iranians and specialists were it not for [the] fact[] [that] **Iran’s security agencies ... are the biggest backers of terrorism in the Middle East**, notably through ... Hezbollah....”³⁸¹
- (vi) Newsweek, June 2004: “While the link to Iran has been publicly known for some time, the 9/11 commission has uncovered evidence that in the mid-1990s Osama bin Laden cast aside religious differences with the Iranians and arranged to have his terror operatives conduct training in explosives and **security at Iranian-backed camps run by Hizbullah in Lebanon**.”³⁸²

³⁷⁷ Holger Jensen, *Sanctions Target Libya, Ignore Other Terrorist Regimes*, Denver Rocky Mountain News (Apr. 16, 1992), (emphasis added), 1992 WLNR 425546.

³⁷⁸ Lance Williams and Erin McCormick, *Bin Laden’s Man in Silicon Valley*, San Francisco Chronicle (Sept. 21, 2001), (emphasis added), 2001 WLNR 5755282.

³⁷⁹ Washington Post (Op-Ed), *The Irony of Iran* (Nov. 11, 2001), (emphasis added), 2001 WLNR 13678266.

³⁸⁰ Matthew Gutman, *Packing Up Our Troubles*, Jerusalem Post (June 28, 2002), (emphasis added), 2002 WLNR 164656.

³⁸¹ Boston Herald (Op-Ed), *Taking First Steps in Iran* (Mar. 21, 2004), (emphasis added), 2004 WLNR 393400.

³⁸² Michael Isikoff and Mark Hosenball, *Terror Watch: Friends of Al Qaeda*, Newsweek Web Exclusives (June 16, 2004), (emphasis added), 2004 WLNR 3641416.

- (vii) *Express on Sunday*, March 2005: “[T]he terrorist group Hezbollah and [] **Iranian security chiefs** ... are **key sponsors of international terrorism**.”³⁸³
- (viii) *AP Worldstream*, August 2006: “State Department spokesman Sean McCormack ... denounced Iran as a **supporter of terror groups** in defiance of U.N. resolution. That support, he said, was ‘**an integral part**’ of Iran’s foreign and national **security policy**.”³⁸⁴
- (ix) *Khaleej Times*, September 2009: “The Middle East Times reported ... that the [U.S.] was stepping up scrutiny of **Iranian security** and military personnel in the Lebanese communities of Latin America. ... US officials said that in addition to boosting rates of recruitment, Hezbollah agents, supported by Iran, are using **very effective routes to smuggle drug profits to the Middle East to aid anti-US counterparts** ...”³⁸⁵
- (x) *Australian*, April 2010: “An ASIO assessment included in the [Australian] federal government's recent counter-terrorism white paper drew attention to the presence in Australia of the Lebanese Hezbollah **External Security** Organisation (ESO), an Iranian-sponsored group described on the federal government's national security website as ‘**among the best-organised terrorist networks in the world**’ ... ASIO pinpointed ESO as a group ‘with a long history of engaging in terrorist acts.’”³⁸⁶
- (xi) *American Forces Press Service*, April 2010: “Defense officials have described the **security threats** posed by Iranian proxies operating in the Middle East -- Hamas in Gaza and Hezbollah in Lebanon -- which the United States and Israel consider terrorist organizations.”³⁸⁷
- (xii) *Reuters*, October 2017: “The Revolutionary Guards (IRGC) are Iran's most powerful internal and external security force.”³⁸⁸

³⁸³ Tim Shipman, *How Real is Terror Threat to Britain?*, *Express on Sunday* (UK) (Mar. 6, 2005), 2005 (emphasis added), WLNR 3482170.

³⁸⁴ Barry Schweid, *U.S. Foresees Further Defiance By Iran To U.N. Demands On Uranium Enrichment*, *AP Worldstream* (Aug. 8, 2006), (emphasis added).

³⁸⁵ *Khaleej Times*, *The Enemy at the Gates - Fear of the Unknown in Latin America* (Sept. 27, 2009), (emphasis added), 2009 WLNR 19020314.

³⁸⁶ *Australian*, *Iranian Embassy ‘Spying on Activist Students’* (Apr. 6, 2010), (emphasis added), 2010 WLNR 7047177.

³⁸⁷ John J. Kruzal, *Gates Satisfied with U.S. Planning to Counter Iran*, *American Forces Press Service*, Defense Department Documents (Apr. 27, 2010), (emphasis added), 2010 WLNR 8757413.

³⁸⁸ *Reuters*, Yedioth Ahronoth (Israel), *Iran Warns US Against Imposing Further Sanctions* (Oct. 8, 2017), (emphasis added), 2017 WLNR 30811998.

9. “Security” Euphemism-Related Media Coverage

1066. Defendants could not possibly have missed the meaning of “security” in their conspiracy with the terrorists because decades of media discussions, television, and film events across a broad array of cultures, religions, and languages in the U.S., Europe, the Middle East, and Africa, where Defendants’ employees and agents live and work, alerted Defendants that “security” was a famously common euphemism for “terrorism,” including, but not limited to:

- (i) Miami Herald, July 1992: “[T]he FMLN has created what the government calls ‘**terror squads**’ *euphemistically* named ‘**security commissions**.’”³⁸⁹
- (ii) Journal of Commerce, November 2002: “The Maritime Transportation Security Act gives us a new *euphemism*. Inside the Beltway, a ‘**terrorist**’ attack’ is now a ‘transportation **security**’ incident.”³⁹⁰
- (iii) Aberdeen American News, June 2004: “‘On the roller coaster ride that Iraq has become, ...[w]hat’s *euphemistically* referred to as ‘**security concerns**’ ... *would be referred to as violent, bloody terrorism* in most other parts of the world.’”³⁹¹
- (iv) Jerusalem Post, August 2004: “‘The term ‘**security** prisoners’ is ... a *euphemism* for ideologically motivated murderers convicted of **terrorist** activities against Israelis.’”³⁹²
- (v) Toronto Star, May 2005: “In an extraordinary trip to Abu Ghraib prison ... she encounters the now-notorious U.S. Army General Janis Karpinski, who tells her that ‘**security** detainees,’ the *euphemism for terrorism* suspects held by the U.S. forces, are ‘relaxed, comfortable, and had everything they need.’”³⁹³
- (vi) Times of India, November 2006: “To paraphrase Chesterton, there are an infinity of angles at which Anglo-Pakistani relations fall but there is only one - **security** - at which

³⁸⁹ Miami Herald, *Peace on a Razor’s Edge* (July 30, 1992), (emphasis added), 1992 WLNR 2253569.

³⁹⁰ R. G. Edmonson, *Washington View: Port Security Bill a Good Start*, Journal of Commerce (Nov. 18, 2002), (emphasis added), 2002 WLNR 1291549.

³⁹¹ Aberdeen American News (SD), *U.N. Vote Brings Glimmer of Hope* (June 10, 2004), (emphasis added), 2004 WLNR 18926896.

³⁹² Efraim Inbar (Professor of Political Studies at Bar-Ilan University), *Let Them Starve*, Jerusalem Post (Aug. 22, 2004), (emphasis added), 2004 WLNR 237090.

³⁹³ Olivia Ward, *Finding Dignity Amid the Chaos; Iraq Journal*, Toronto Star (May 22, 2005), (emphasis added), 2005 WLNR 8118912.

they stand. *The ‘S’ word is a euphemism for the ‘T’ word. Terrorism, as sponsored by Pakistan.*”³⁹⁴

- (vii) *New American*, April 2008: “Lieutenant General Keith Dayton, the Bush administration’s Security Coordinator for Palestine, testified ... on the supposed need to fund President Abbas’ *‘security forces,’ a euphemism for the collection of terrorist thugs* from the al-Aqsa Martyrs Brigades, Islamic Jihad, Force 17, and various other PLO/Fatah militias.”³⁹⁵
- (viii) *Birmingham Post*, October 2008: “[A]n event ... sought to consider *‘security and community cohesion’ a euphemism for extremism and terrorism, natch*.”³⁹⁶
- (ix) *BBC International Reports (Latin America)*, October 2013: “Although paramilitary forces could serve the interests of the State, its members act as mercenaries, assault squads, thugs, and private *security groups*, the latter a *euphemism for terrorists*.”³⁹⁷
- (x) *Electronic Intifada (Palestine)*, August 2021: “The term ‘ISF’ – which stands for ‘Israeli security forces’ – is a total misnomer and euphemism for occupation forces who provide anything but ‘security.’ Their job, rather, is to terrorize and repress.”³⁹⁸
- (xi) *Canada Stockwatch*, September 2014: “[I]n the Democratic Republic of the Congo ... a ... *‘security incident[]’* ... is one of several *euphemisms for an ‘act of terror,’* ‘war,’ or even a spontaneous hacking.”³⁹⁹

³⁹⁴ Rashmee Roshan Lal, *TomKat Nuptials Like Blair-Mush Compact*, Times of India (Nov. 19, 2006), (emphasis added), 2006 WLNR 27474749.

³⁹⁵ William F. Jasper, *A Bad Investment: U.S. Support For So-Called “Moderate” Terrorists as the Alternative to Worse Terrorists, as we have Given in Palestine, is a Recipe for Disaster*, New American (Apr. 28, 2008), (emphasis added), 2008 WLNR 25511423.

³⁹⁶ Chris Allen, *Freedom of Expression is Built on the Right to Offend*, Birmingham Post (UK) (Oct. 16, 2008), (emphasis added), 2008 WLNR 19647906. “Natch” means “naturally; as may be expected.”

³⁹⁷ BBC International Reports (Latin America), *Costa Rican Daily Warns Caution Over Alleged Presence of Paramilitary Group* (Oct. 3, 2013), (emphasis added).

³⁹⁸ Electronic Intifada (Palestine), *Video Shows Israeli Shooting That Killed 11-Year-Old Boy* (Aug. 4, 2021), 2021 WLNR 25165762. Plaintiffs categorically reject the antisemitic bile displayed in this quotation and offer it merely to show the widespread euphemistic use of “security.”

³⁹⁹ Canada Stockwatch, **MKTDIAM Diamonds & Specialty Minerals Summary for Sept. 22, 2014* (Sept. 22, 2014), (emphasis added).

10. Each Defendant's or Co-Conspirator's Consciousness of Guilt

1067. The conduct of MTN Group, MTN Dubai, MTN Group's President and CEO, MTN Group's Commercial Director, ZTE Corporation, ZTE USA's in-house attorney, Huawei Co., Huawei Co.'s CFO, and others compels the conclusion that each Defendant knew that "security" was a euphemism for the external terror operations of Hezbollah, the Qods Force, and Regular IRGC. Each Defendant manifested obvious **consciousness of guilt** concerning their relationship with the Iranian Shareholders:

- (i) **MTN Group's President and CEO** concealed the secret agreement from MTN Group's shareholders, Board of Directors, outside counsel, auditors, as well as various governments including, on information and belief, the U.S. government and the South African government.
- (ii) **ZTE Corp.**, and its internal legal department, also showed consciousness of guilt because it created internal memoranda intended to guide a company-wide scheme to evade U.S. sanctions to get embargoed U.S.-origin technology to Iran and oversaw a cover-up campaign designed to destroy and distort evidence of its criminal wrongdoing. When the ZTE USA general counsel learned of the company-wide scheme, he became a whistleblower that spawned massive criminal investigations, prosecutions, and fines.
- (iii) **Huawei Co.** showed consciousness of guilt because it devised a scheme to conceal its role in sourcing embargoed U.S.-origin goods and services to Iran, while directing its officers, including its CFO, to make multiple material misrepresentations to U.S. authorities and financial institutions to conceal the scope and nature of its Iranian business. Further, when Huawei learned of the U.S. government's investigations concerning Huawei's Iranian interests, Huawei Co. ordered its employees, and the employees of its subsidiaries, including Huawei Device USA, to destroy documentary evidence and remove witnesses outside the jurisdiction of the U.S. authorities.

1068. Defendants' consciousness of guilt can **only** be explained by each Defendants' knowledge that the IRGC's "security" assistance needs comprised knowingly providing material support for the terrorist agenda of Hezbollah, the Qods Force, and Regular IRGC for the specific purpose of facilitating the anti-American terror "security" operations of Hezbollah, the Qods Force, and Regular IRGC: (a) **inside of Iran**, e.g., joint training camps funded by the IRGC and staffed by Hezbollah, through which the IRGC's Shiite Terrorist Proxies and Sunni Terrorist

Proxies received essential training, safe haven, and logistical support designed to facilitate their terrorist attacks against Americans in Afghanistan, Iraq, Syria, Yemen, Israel, and Europe; and (b) **outside of Iran**, including, but not limited to, through IRGC proxies in Afghanistan, Iraq, Syria, Yemen, Israel, and Europe e.g., a Joint Cell in Basra that specializes in kidnapping and was comprised of Hezbollah, the Qods Force, and Jaysh al-Mahdi, as well as a Joint Cell in Syria that provides communications and smuggling support for the IRGC's Shiite Terrorist Proxies.

1069. This conclusion is ineluctable for several reasons. With respect to the phrase “defensive, security, and political cooperation,” two of those three items were unquestionably legal in Defendants’ home countries. At all relevant times, South African and Chinese companies could legally sell weapons to Iran, and therefore it is implausible that Defendants were worried about the criminal risk of facilitating weapons sales from South Africa because however disgusting such conduct was, it was not illegal under South African law (and MTN Group did not have any U.S. affiliates).

1070. Moreover, the South African and Chinese governments were both longstanding close allies of Iran based upon their unique historical bonds, and in such context, it is implausible that Defendants were concerned about breaking the law by promoting “political cooperation” between their respective countries and Iran, since “political cooperation” with Iran was a perfectly acceptable thing in both South Africa and China at all relevant times.

1071. **Only** Defendants’ knowledge that “security” meant “Hezbollah, Qods Force, and anti-American terror” explains the totality of each Defendant’s conduct, as well as the parallel nature of their crimes, e.g., rampant document destruction. For Defendants to facilitate a helicopter sale to the regular Iranian Army (not the IRGC), or help broker political cooperation, was not only legal, but in furtherance of the economic and political agendas of all but the U.S.

Manufacturer Defendants' home countries, South Africa and China. For Defendants to agree to provide "security assistance" to the IRGC (including Hezbollah and the Qods Force), however, was a categorically different matter.

1072. With respect to MTN Group and MTN Dubai, directly assisting the "security" operations of Hezbollah, the Qods Force, and Regular IRGC plainly ran the risk of committing a litany of crimes under South African law (e.g., terrorism crimes and espionage), and created obvious – and dire – potential risk to any MTN Group or MTN Dubai executive, employee, or agent who participated in the conspiracy without making a noisy withdrawal. Indeed, to this date, MTN Group and MTN Dubai have yet to exit the conspiracy.

1073. With respect to ZTE and Huawei, the motivation to conceal their direct "security" assistance to the IRGC was rooted in an obvious explanation: both sought to facilitate the hostile activities of the Chinese Communist Party that aided the IRGC's Shiite Terrorist Proxies and the IRGC's Sunni Terrorist Proxies in order to facilitate attacks against targeted Americans in Afghanistan, Iraq, and throughout the Middle East to drive the U.S. out so that China could become the dominant regional power consistent with the ideology and agenda of the Chinese Communist Party.

C. Defendants Knew Their Illicit Transfers Of Cell Phones To Hezbollah, The Qods Force, And Regular IRGC Aided the Conspiracy's Terrorist Attacks Against Americans Worldwide

1074. Defendants knew that their illicit provision of American smartphones, computing technologies, and other key items requested by Hezbollah, the Qods Force, and Regular IRGC was an act of international terrorism because Defendants knew that such phones, supplied in such volumes to such terrorists, would fund, and logistically support, thousands of terrorists every year.

1075. Defendants knew that Hezbollah, the Qods Force, and IRGC proxies like al-Qaeda, depended upon reliable supplies of cell phones as a key growth engine for expanding the shared global terrorist enterprise they needed to effectively counter the U.S. and NATO and kill Americans in Afghanistan and Iraq. For example, as the *Montreal Gazette* reported at the time:

Under [] Ahmadinejad [], U.S. officials said, the [IRGC] has moved increasingly into commercial operations, *earning profits* and extending its influence in Iran in areas involving big government contracts, including ... *providing cell phones*. Washington has claimed the Revolutionary Guard's Quds Force wing is responsible for the growing flow of explosives, roadside bombs, rockets and other arms to Shiite militias in Iraq and the Taliban in Afghanistan. Quds Force has also been blamed for supporting Shiite allies such as Lebanon's Hezbollah and to such Sunni movements as Hamas and the Palestinian Islamic Jihad.⁴⁰⁰

1076. Defendants knew that, since 9/11, *every* major transnational Islamist terrorist organization that has targeted Americans has prioritized providing its operatives have a robust, reliable, and covert supply of two material items above all else: stockpiling vast quantities of secure, untraceable American mobile phones, and obtaining as much U.S. currency as possible. This maxim holds true for Shiite and Sunni groups alike, including, but not limited to, the IRGC (including Hezbollah and the Qods Force) Jaysh al-Mahdi, al-Qaeda, the Taliban (including its Haqqani Network), ISIS, al-Nusra Front, and every other major group.

1077. Decades of media coverage alerted Defendants to Hezbollah's specific reputation for using cell phones to help commit terrorist violence, including, but not limited to:

- (i) *L.A. Times*, November 1997: "Hezbollah us[ed] *mobile phones to coordinate attacks* and roadside bombs camouflaged as rocks."⁴⁰¹
- (ii) *Montreal Gazette*, March 2001: "Two men ... were accused of aiding the Islamic extremist group Hezbollah in an indictment ... They are said to have conspired to provide

⁴⁰⁰ *Montreal Gazette* (Canada), *What is the Revolutionary Guard?* (Aug. 16, 2007), 2007 WLNR 28659733.

⁴⁰¹ Marjorie Miller, *Hezbollah Battles to Shed Extremist Image in Lebanon*, *Los Angeles Times* (Nov. 28, 1997) (emphasis added), 1997 WLNR 5640765.

Hezbollah with cash, night-vision goggles, global-positioning devices, mine-detection equipment, **cell phones** and blasting equipment.”⁴⁰²

- (iii) *Globe & Mail*, July 2006: “Air strikes took out relay towers belonging to Lebanon's three main cellular phone companies, Hezbollah's al-Manar television network ... Such communications channels are traditional targets ahead of military action.”⁴⁰³
- (iv) *Detroit Free Press*, July 2006: “Capt. Jacob Dallal, an Israeli army spokesman, said the targets of the strikes were Al-Manar and Al-Nour, Hizballah's TV and radio stations, respectively. He said five of the radio station's antennas were hit. ‘It's important to understand why the attack was carried out,’ Dallal said. ‘This will disrupt their ability to communicate,’ he said, adding that **cell phones were a ‘key communication link’ for Hizballah.**”⁴⁰⁴
- (v) *Daily Mail*, November 2007: “Back at base, [Chris] Hunter [a “veteran 'ammunition technical officer' or counterterrorist bomb-disposal expert”] looks for patterns in the way that bombs are made and laid. At first his main opponent is a Sunni bomb-making gang, who are happy to slaughter scores of Shia civilians along with Coalition soldiers. Then, in the spring of 2004 comes the Shia militia uprising. **They increasingly receive high-tech help from Iran and even Lebanese Hezbollah in using devices such as mobile phones to detonate bombs by remote control.**”⁴⁰⁵
- (vi) *Washington Times*, March 2009: “Almost everyone I met warned me about using my cell phone. It was **common knowledge that Hezbollah officers in the security forces were regularly intercepting phone calls and tracking their human targets** by triangulating the signals the phones send out to cell phone towers around the city.”⁴⁰⁶
- (vii) *Derby Evening Telegraph*, November 2009: “Mr Godsmark told the jury that a video clip found on an external hard-drive at Lusha's home gave instructions on how to turn a mobile phone into a bomb trigger. The prosecutor also said video clips produced by organisations undertaking “fundamentalist violent jihad in Iraq, Afghanistan and Chechnya ... Mr Godsmark said 14 mobile phones were also found at Lusha's home. Documents found on computers or drives include the Hezbollah Military Instruction

⁴⁰² Montreal Gazette (Canada), *B.C. Men Accused of Aiding Hezbollah* (Mar. 29, 2001) (emphasis added), 2001 WLNR 6561271.

⁴⁰³ Carolynne Wheeler, *Israeli Troops Enter Village in Lebanon*, globeandmail.com (Toronto), (July 22, 2006), 2006 WLNR 27225853.

⁴⁰⁴ Detroit Free Press, *Israeli Push Deepens Conflict* (July 23, 2006) (emphasis added), 2006 WLNR 25249492.

⁴⁰⁵ Jonathan Foreman, *Defusing the Iraqi Conflict*, Daily Mail (UK) (Nov. 2, 2007) (emphasis added), 2007 WLNR 21680052.

⁴⁰⁶ Kenneth Timmerman, *Fear Grips Democracy in Lebanon*, Washington Times (Mar. 2, 2009) (emphasis added), 2009 WLNR 4034008.

Manuals; Middle Eastern Terrorist Bomb Design; Improvised Radio Detonation Techniques; Radnar's Detonators; The Mujahideen Explosives Handbook and The Bomb Book. A video film entitled "mobile detonators" was also discovered."⁴⁰⁷

1078. Indeed, Defendants were alerted by Hezbollah's own public statements taunting the United States concerning a purported "US 'request' for information on mobile phones."⁴⁰⁸

D. Defendants Knew That Their Protection Payments To The Taliban, Including Its Haqqani Network, Facilitated Terrorist Attacks By Al-Qaeda And The Taliban Against Americans In Afghanistan And Were Opposed By The U.S. Government For That Reason

1. Defendants Knew That Their Cash And "Free Goods" Protection Payments To The Taliban, Including Its Haqqani Network, Financed, Armed, And Logistically Sustained Terrorist Attacks By Al-Qaeda And The Taliban Against Americans In Afghanistan

1079. Defendants knew (or recklessly disregarded) that they were supplying funding to Taliban terrorists intent on attacking Americans in Afghanistan. The Taliban openly proclaimed that the money was for terrorism: as the Taliban told one subcontractor in a typical example, "You know we need this American money to help us fund our Jihad."⁴⁰⁹ The demands for payments, which the Taliban itself tied to the insurgency, alerted Defendants to the connection between the payments and insurgent violence. As one security firm that faced demands for protection money acknowledged in a November 2007 memorandum, it was obvious that "[i]f we make payment that money will be funneled back into [the Taliban's] fight against the Coalition."

⁴⁰⁷ *Id.*

⁴⁰⁸ Al-Sharq al-Awsat, BBC International Reports (Middle East), *Lebanese Hezbollah Reacts to US "Request" For Information on Mobile Phones* (Mar. 3, 2010) ("Lebanese Hezbollah reacts to US "request" for information on mobile phones. Accusations against the US Embassy in Beirut that it seeks to obtain sensitive information on the mobile phone networks raised doubts within Hezbollah. Hezbollah has doubts that this information might be used by the US intelligence in infiltrating the communications network and tracking Lebanese figures.").

⁴⁰⁹ *Afghan Firms Pay Off Taliban.*

1080. Defendants also negotiated their payments in circumstances that left no doubt about whom they were financing. With respect to the large-scale payments negotiated directly with the Quetta Shura, Defendants (or their agents) met with high-level Taliban representatives who openly represented the Taliban's Financial Commission. The payments to local Taliban officials likewise occurred via negotiations with commanders or shadow "governors" who openly identified as Taliban members. Given the Taliban-controlled geographies in which Defendants operated, Defendants assuredly knew (or recklessly disregarded) that the officials they were paying off worked for the Taliban.

1081. The Taliban memorialized its protection racket in documents that further notified Defendants that they were financing terrorists. Most prominently, the Taliban often conveyed its demands for protection payments in so-called "Night Letters." Night Letters – whose name comes from their frequent delivery during the night – were documents on official Taliban letterhead bearing the Taliban's insignia. Although Night Letters could convey a variety of threats, the Taliban commonly sent them to companies to demand protection payments. One typical example, delivered to phone companies in Wardak Province, stated that "we are expecting you to provide financial support for the Taliban stationed in Saidabad district. If you cannot, then you should stop your work. Otherwise you have no right to complain in the future (we are warning you of future incidents)." Another, authored by the "Islamic [Emirate] of Afghanistan" (the Taliban's formal name for itself), informed a local construction company that it "cannot continue to work unless it does obtain permission from the Mojahedeen. Or else, it does not have the right to complain." Night Letters were widespread in Afghanistan, particularly in areas of Taliban control, and were one of the principal means through which the Taliban communicated its demands for protection money to companies, including Defendants.

1082. Similarly, after effecting the payments, companies regularly received so-called “tax receipts” from the Taliban, providing them with documentation proving they had paid their dues to the insurgents. The Taliban Financial Commission encouraged the provision of tax receipts as a way of further standardizing and accounting for the revenue raised through the insurgents’ protection rackets. And those tax receipts – like the Night Letters – appeared on Taliban letterhead and made clear on their face that protection money was intended for the Taliban’s benefit. On information and belief, Defendants or their agents received Night Letters and Taliban tax receipts in connection with their projects in Afghanistan.

1083. Defendants did not believe – nor was it true – that their payments were necessary for them to avoid imminent death or serious bodily injury. The Taliban typically did not extract protection payments by physically confronting companies and threatening immediate violence; rather, the threats were often vaguer and futuristic – as in the Night Letters mentioned above. Many times, those threats were directed at Defendants’ equipment or projects, rather than their personnel. Given the non-immediate nature of the threats, Defendants could notify the U.S. government of the Taliban’s protection racket and try to enlist the military’s assistance in responding. But rather than avail themselves of such options, Defendants decided that the simplest (and most profitable) option was to make the payments the Taliban demanded.

1084. Defendants’ practice of funneling many (though far from all) of their payments through subcontractors, only heightens their culpability. Defendants intentionally used the contracting process to insulate themselves from the payments on paper, but that process – offloading responsibility to local subcontractors several layers removed – was simply their technique for encouraging the payments while avoiding responsibility. The payments may often have been physically delivered by an intermediary, but Defendants knew they were occurring

and purposefully orchestrated them. That is because Defendants could only obtain their desired business outcome by ensuring that their money actually reached the Taliban. Had Defendants' subcontractors spent the money on some other, legitimate purpose, rather than directing it to the Taliban, Defendants would not have obtained the security benefit they wanted.

1085. Western contractors have confirmed their understanding that, during the relevant timeframe, local intermediaries were routing contract money to the Taliban on their behalf. The head of one private-security company admitted that his “boss wouldn’t appreciate it if I went to negotiate face to face with the tribal leaders of Helmand” – historically a key part of Taliban leadership – so he instead used “intermediaries who recruit our security guards locally.”⁴¹⁰ Exemplifying the no-questions-asked mentality typical of many contractors, the executive stated, “You just hope they’re not linked too closely with the Taliban.”⁴¹¹

1086. Another contractor negotiating a shipment of pipes through Helmand confirmed to a reporter that he typically “tacked on about 30 percent extra for the Taliban,” which he accounted for as “transportation costs” charged back to the prime contractor running the project.⁴¹² When the “foreign contractor in charge of the project” was asked about it, the contractor admitted, “We assume that our people are paying off the Taliban.”⁴¹³

1087. Yet another American contractor admitted that his protection payments – amounting to 16% of his gross revenues – were “all revenue that will ultimately be shared by the Taliban.”⁴¹⁴ This contractor was well aware of the consequences: “‘All of this could be seen as

⁴¹⁰ *Taliban’s Secret Weapon*.

⁴¹¹ *Id.*

⁴¹² *Funding The Afghan Taliban*.

⁴¹³ *Id.*

⁴¹⁴ *How The Taliban Thrives* at 50.

material support for enemy forces,’ he muse[d]. ‘But you have to weigh that against everything that is being done in that project. Are you aiding and abetting the enemy if you have to pay to get a school built? It’s the cost of doing business here.’”⁴¹⁵

1088. By no later than 2008, Chinese media reports specifically alerted Defendants that the Taliban, including its Haqqani Network, relied upon communications technologies to conduct attacks against Americans in Afghanistan. For example, on February 25, 2008, *Xinhua News Agency*, which is a Chinese Communist Party analogue to the Associated Press, reported that the “Taliban threaten[ed] Afghan mobile telecom companies,” which alerted Defendants to the Taliban’s communications technology rackets in Afghanistan.⁴¹⁶

1089. At all relevant times, it was common knowledge among businesses operating in Afghanistan, including Defendants, that Western contracting dollars were flowing to the Taliban in the form of protection money. Because the Taliban openly demanded the money – and because local subcontractors openly paid it – companies on the ground in Afghanistan were widely aware of the practice. One journalist referred to such payments as an “open secret”⁴¹⁷; another called protection payments a “widely known practice in Afghanistan”⁴¹⁸; and experts described it to *CBS News* as an “open secret on the streets.”⁴¹⁹ Defendants were sophisticated companies with millions of dollars in revenues on the line in Afghanistan. They were aware of this prevailing understanding that their “security” payments were flowing to the Taliban.

⁴¹⁵ *Id.*

⁴¹⁶ Xinhua News Agency, *Taliban Threatens Afghan Mobile Telecom Companies* (Feb. 25, 2008).

⁴¹⁷ *Funding The Afghan Taliban*.

⁴¹⁸ Dana Chivvis, *Is The Taliban Getting A Cut Of U.S. Aid?*, CBS News (Sept. 3, 2009).

⁴¹⁹ Nancy Cordes, *Is Taxpayer Money Funding The Taliban?*, CBS News (Sept. 3, 2009).

1090. A *Time Magazine* cover story on September 7, 2009, entitled “Taliban Inc. – How Drugs, Extortion, Protection Rackets And Foreign Aid Fuel The Afghan Insurgency,” accompanied a full-page cover graphic depicting an AK-47 lying on top of a box full of \$100 bills. In the article, the author noted that “protection payments are so widespread that one contractor I interviewed responded incredulously to questions about how the system worked. ‘You must be the only person in Afghanistan who doesn’t know this is going on,’ he said.”⁴²⁰

1091. Throughout the relevant timeframe, accounts from other prominent media sources also reported that contractors and subcontractors were redirecting Western contract funds to the Taliban. Those widespread reports further informed Defendants that their expenditures in Afghanistan were delivering protection money to the Taliban. Examples include:

- (i) *BBC International Reports (Europe)*, October 2004: “[T]he merging of organized crime and terrorism is a new phenomenon. BND President Hanning assumes ‘that terrorist structures, such as ***the Taleban and Al-Qa’idah, finance their fight through the extortion of protection money*** as well as direct involvement in drug-trafficking.’”⁴²¹
- (ii) *National Post (Canada)*, September 2006: “The Taliban still have a partnership with al-Qaeda, which provides them training and foreign fighters. If they have it their way, Afghanistan would once again be a hot-house of terrorism. Today, ***the Taliban is*** also in league with drug lords, protecting the crop, ***taking protection money like any mafia***, and using that money to fund their insurgency.”⁴²²
- (iii) *Times Record News*, August 2008: “The Taliban tried a similar cell phone tower extortion racket, but it backfired. StrategyPage reported on June 15 that ***the Taliban were expanding ‘their extortion campaign, demanding that businesses pay “protection money” to avoid being attacked’*** and an effort by the Taliban ‘to control cell phone use has quickly evolved into just another extortion campaign.’ . . . ‘But then, noting that there were several cell phone companies operating in southern Afghanistan, ***the Taliban***

⁴²⁰ *How The Taliban Thrives* at 50.

⁴²¹ BBC International Reports (Europe), *German Intelligence Chief Says Bin-Ladin Still Alive* (Oct. 10, 2004). All emphases in this paragraph are added.

⁴²² Jaap de Hoop Scheffer, *The World Can Do More: NATO’s Secretary-General On What Afghanistan Needs*, *National Post* (Sept. 13, 2006), 2006 WLNR 26238821.

*went to the different companies and offered not only “protection,” but damage to a competitor, for a price.’”*⁴²³

- (iv) *Inter Press Service*, September 2008: “Often petrol delivery and logistics companies have to pay protection money to various tribal elders. In one route, between the capitals of Kandahar and Urozgan provinces, **contractors pay millions in protection money, some of which may end up in the hands of the Taliban**, [Matthew] Leeming says.”⁴²⁴
- (v) *Hindustan Times*, December 2008: “NATO convoys carrying military supplies for NATO bases in South Afghanistan, are reported **paying Taleban commanders protection money to ensure safe passage**. . . . The Times has learnt that it is the outsourcing of convoys that [leads to] payoffs amounting to millions of pounds, including money from British taxpayers, are given to the Taleban. Several fuel importers, trucking and security company owners confirmed the controversial payments.”⁴²⁵
- (vi) *Deutsche Presse Agentur*, June 2009: “Afghanistan’s private sector does its share to finance the insurgency – albeit not entirely voluntarily. **Those who want to do business in the south have to pay protection money to the Taliban**. According to businessmen, even the international troops indirectly put money in the insurgents’ war chest . . . ‘Everything has to do with money,’ said [Khalid] Naderi, who co-owns a telecommunications firm that operates in the restive south, where he pays \$2,000 in protection money per month for each of his transmission masts. ‘You have to do it. Everybody does.’”⁴²⁶
- (vii) *Frankfurter Rundschau* (Germany), July 2009: “**In the cases of major projects**, contractors have to have the construction plans and bidding documents scrutinized by Taleban engineers after which **the amount of the charge is fixed**.”⁴²⁷
- (viii) *Time Magazine*, September 2009: “[Sargon] Heinrich says some 16% of his gross revenue goes to ‘facilitation fees,’ mostly to protect shipments of valuable equipment coming from the border. ‘**That is all revenue that will ultimately be shared by the Taliban**.’ . . . In fact, **protection payments are so widespread** that one contractor I interviewed responded incredulously to questions about how the system worked. ‘**You must be the only person in Afghanistan who doesn’t know this is going on**,’ he said.”⁴²⁸
- (ix) *Star-Ledger*, September 2009: “The United States Agency for International Development has opened an investigation into allegations that its **funds for road and**

⁴²³ Times Record News, *Anatomy Of Terror* (Aug. 21, 2008), 2008 WLNR 31329261.

⁴²⁴ Anand Gopal, *Afghanistan: Subsidised Fuel Trail Winds Back To Pakistan*, *Inter Press Service* (Sept. 30, 2008).

⁴²⁵ *Hindustan Times*, *NATO Convoys Paying Taleban Protection Money For Safe Passage In Afghanistan* (Dec. 12, 2008), 2008 WLNR 23872308.

⁴²⁶ *How The Taliban Has Turned Extortion Into A Gold Mine*.

⁴²⁷ Willi Germund, *Steuergeld für Taliban*, *Frankfurter Rundschau* (July 1, 2009) (quoted by Thomas Ruttig, *The Other Side* at 20-21, Afghanistan Analysts Network (July 2009)).

⁴²⁸ *How The Taliban Thrives* at 50.

bridge construction in Afghanistan are ending up in the hands of the Taliban, through a protection racket for contractors. And a House Foreign Affairs Committee member, Rep. Bill Delahunt (D-Mass.), vowed to hold hearings on the issue in the fall, saying: ‘The idea that American taxpayer dollars are ending up with the Taliban is a cause for grave concern.’”⁴²⁹

- (x) *Sunday Telegraph*, September 2009: “*A far larger source of Taliban income, however, are the protection rackets by which they siphon off a significant part of the billions of dollars* we and other Western countries pour into Afghanistan to keep troops supplied and to provide new infrastructure, such as schools and roads, under a multiplicity of aid programmes.”⁴³⁰
- (xi) *Sydney Morning Herald*, September 2009: “The Taliban also keep an eye on local individuals who get work on the project – especially those doing the all-important security jobs. . . . *Deals in which the Taliban top up their coffers by demanding as much as 30 per cent of the value of a contract as protection money are rife.*”⁴³¹
- (xii) *The Independent*, March 2010: “[The investigation] is prompted by mounting concerns that *the very money supposed to win over the hearts and minds of Afghans is ending up in the hands of the Taliban*, drug lords or profiteers. The British commander’s concern is part of a wider crackdown on corruption, with General Stanley McChrystal having declared war on those making millions out of what has become a billion-dollar black hole for aid funds, in an anti-corruption directive issued last month. A third of the costs of supplying the armed forces in Afghanistan is spent on paying protection, bribery and safe passage.”⁴³²
- (xiii) *Washington Post*, March 2010: “According to senior Obama administration officials, *some of [the money] may be going to the Taliban, as part of a protection racket* in which insurgents and local warlords are paid to allow the trucks unimpeded passage, often sending their own vehicles to accompany the convoys through their areas of control. The essential question, said an American executive whose company does significant work in Afghanistan, is ‘whether *you’d rather pay \$1,000’ for Afghans to safely deliver a truck, even if part of the money goes to the insurgents*, or pay 10 times that much for security provided by the U.S. military or contractors.’”⁴³³
- (xiv) *New York Times*, June 2010: “For months, *reports have abounded here that the Afghan mercenaries* who escort American and other NATO convoys through the badlands *have been bribing Taliban insurgents* to let them pass. . . . Although the investigation is not complete, the officials suspect that at least some of these security companies – many of

⁴²⁹ *U.S. Aid Helps Fund Taliban.*

⁴³⁰ *How We Help To Arm The Taliban.*

⁴³¹ *Insurgents Play A Perilous Mountain Game.*

⁴³² *Army Launches Investigation.*

⁴³³ *Afghan Corruption.*

which have ties to top Afghan officials – are *using American money to bribe the Taliban*.⁴³⁴

- (xv) *The Guardian*, June 2010: “Private haulage companies that carry vital supplies to American soldiers in Afghanistan have *helped to fund the Taliban and fuel ‘a vast protection racket* run by a shadowy network of warlords,’ according to a US congressional report.”⁴³⁵
- (xvi) *NPR*, June 2010: “In fact, a lot of the money is already being wasted because we, the international community, is donating tens of billions of dollars to aid Afghanistan. But what happens when contractors go out to build hospitals or other projects? *They wind up paying off the Taliban protection money. So in effect, the international aid winds up subsidizing the enemy.* That is what’s going on right now.”⁴³⁶
- (xvii) *Washington Post*, July 2010: “Contracting officials, under heavy pressure to produce results, often favor efficiency over all other factors, military officials said. A recent report by a House oversight subcommittee concluded that *tens of millions of dollars* spent to protect U.S. military supply convoys traveling through dangerous parts of the country *went to local warlords, listed as ‘subcontractors,’ in the form of protection money. Some of the funds*, the report concluded, *likely went to the Taliban*.”⁴³⁷
- (xviii) *Los Angeles Times*, October 2010: “The report, released Thursday by the inspector general of the U.S. Agency for International Development, says *subcontractors* hired to protect a development project near Jalalabad *may have paid more than \$5 million to the militants* through local authorities. . . . The report says local *authorities often demand a 20% ‘protection tax’* in such circumstances. Under those deals – along the lines of extortionist protection rackets in the U.S. – *the Taliban sends security guards with promises that they won’t attack the subcontractors* or their equipment and won’t try to halt the contract work, the report says.”⁴³⁸
- (xix) *Hindustan Times*, October 2010: “About one billion dollars worth of *U.S. aid has wound up in the hands of the Taliban* and other insurgency groups, war analysts and government auditors say. *Sub-contractors have reportedly diverted the funds* from programs meant to stabilize Afghanistan. In fact, the auditors say, graft has gotten so bad

⁴³⁴ Dexter Filkins, *Convoy Guards In Afghanistan Face An Inquiry*, N.Y. Times (June 6, 2010).

⁴³⁵ Jon Boone, *Afghanistan Haulage Contract Helping To Fund Taliban, Says US Report*, The Guardian (June 22, 2010).

⁴³⁶ *The Way Forward In Afghanistan Post-McChrystal*, National Public Radio, Talk of the Nation (June 24, 2010) (statement of Max Boot), 2010 WLNR 12796179.

⁴³⁷ Karen DeYoung, *Afghan War Funds Face New Scrutiny Program To Spur Local Businesses May Instead Benefit Power Brokers*, Wash. Post (July 30, 2010), 2010 WLNR 26709005.

⁴³⁸ Paul Richter, *Audit: U.S. Government Funds May Have Gone To Taliban*, L.A. Times (Sept. 30, 2010).

that the U.S. government estimates that only about 10 percent of the aid budget actually reaches the people in Afghanistan who need it.”⁴³⁹

- (xx) Christian Science Monitor, October 2010: “The Senate investigation also turned up mounting evidence to suggest that largely unmonitored Pentagon ***contracts with private security companies*** – half of which are Afghan-owned – ***may also be lining the pockets of Taliban insurgents*** who agree not to attack convoys in exchange for cash. ‘***If you want to know the driving force of corruption*** in Afghanistan, it’s not Afghan culture,’ warns Anthony Cordesman, a security specialist at the Center for Strategic and International Studies in Washington. ‘***It’s American contracting.***’”⁴⁴⁰
- (xxi) Fox News, October 2010: “And that, she says, has ***formalized a massive protection industry that is run, in many but not all cases, by the Taliban.*** ‘We should be surprised not that convoys are attacked, but by how few get attacked,’ Fair said. That is the same assessment that Richard Holbrooke, the special envoy for Afghanistan and Pakistan, gave to President Obama more than a year ago, according to Bob Woodward’s book, *Obama’s Wars*. ‘***All the contractors for development projects pay the Taliban for protection and use of the roads, so American and coalition dollars help finance the Taliban,***’ Woodward wrote.”⁴⁴¹
- (xxii) The Australian, December 2010: “Roads and buildings have been contracted to favoured Western companies which cream off profits, then sub-contract to local businesses to do the work. These then sub-sub-contract again to even cheaper local firms . . . To protect themselves, the convoy owners hire local security companies. In many instances ***the security firms then pay off the Taliban not to attack. In such situations, Western taxpayers are effectively funding the Taliban.***”⁴⁴²
- (xxiii) New York Times, May 2011: “Critics say that ***payoffs to insurgent groups***, either directly or indirectly, ***by contractors*** working on highways and other large projects in Afghanistan ***are routine.*** Some ***officials say they are widely accepted in the field as a cost of doing business,*** especially in areas not fully under the control of the United States military or the Afghan government.”⁴⁴³
- (xxiv) Washington Post, August 2011: “The U.S. military has moved to ***stem the flow of contract money to Afghan insurgents***, awarding at least 20 companies new contracts worth about \$1 billion for military supply transport and suspending seven current

⁴³⁹ *About A Billion Dollars Worth of US Aid Diverted.*

⁴⁴⁰ Anna Mulrine, *Rogue Security Companies Threaten US Gains In Afghanistan War*, *Christian Sci. Monitor* (Oct. 21, 2010).

⁴⁴¹ Ed Barnes, *Up To \$1 Billion In U.S. Aid Winds Up In Taliban Coffers*, *Fox News* (Oct. 22, 2010) (“*Up To \$1 Billion In U.S. Aid Winds Up In Taliban Coffers*”).

⁴⁴² Tom Coghlan, *Aid Robs Afghan & Iraqi Poor, Helps Rich*, *The Australian* (Dec. 29, 2010), 2010 WLNR 25517589.

⁴⁴³ Alissa J. Rubin & James Risen, *Costly Afghanistan Road Project Is Marred By Unsavory Alliances*, *N.Y. Times* (May 1, 2011) (“*Afghanistan Road Project Marred By Unsavory Alliances*”).

subcontractors it found lacking in ‘integrity and business ethics.’ . . . Congressional investigators determined last year that ***much of the transport and security money went to the Taliban*** and Afghan warlords as part of a protection racket to ensure the safe arrival of the convoys, conclusions that were confirmed this spring by military and intelligence inquiries.”⁴⁴⁴

- (xxv) *The Oregonian*, September 2011: “Most galling of all is that after the illegal drug trade, the ***single largest source of funding*** to Afghan insurgents – our enemy – is the ***extortion of ‘protection’ money*** from U.S.-backed transportation and construction contractors.”⁴⁴⁵
- (xxvi) *Agence France Presse*, September 2012: “‘***Revenue extorted from nationwide enterprises*** such as narcotics producers and traffickers, construction and trucking companies, mobile telephone operators, mining companies[,] and aid and development projects ***goes to the Taliban Financial Commission*** which answers to the Taliban leadership,’ said the report. . . . The sanctions experts said the Taliban have made foreign development funds a ‘lucrative source’. ‘***Estimates of Taliban income from contracts funded by the United States and other overseas donors range from 10 percent to 20 percent*** of the total, usually by the Taliban agreeing protection money with the contractor or demanding a cut.’”⁴⁴⁶
- (xxvii) *The Hindu*, September 2012: “[C]ontractors in Afghanistan often ***say they have to make payoffs of between 10 and 20 percent to ensure work can go ahead.*** In Farah, local officials have claimed that the payoffs are as high as 40 per cent.”⁴⁴⁷

1092. On information and belief, Defendants were aware of these reports or similar ones, and their substance, which documented how protection payments made by Western contractors and subcontractors financed the Taliban’s terrorist attacks. Defendants are sophisticated companies, all of which specialize in performing work in high-risk countries like Afghanistan. Given their business models, and the contractual role they undertook to monitor the local security environment, Defendants each monitored open-source reporting on the risks of

⁴⁴⁴ Karen DeYoung, *U.S. Awards Contracts In Afghanistan*, Wash. Post (Aug. 16, 2011), 2011 WLNR 16187412.

⁴⁴⁵ *The Oregonian*, *Losing \$60 Billion To Fraud & Waste* (Sept. 7, 2011), 2011 WLNR 17729205.

⁴⁴⁶ *Agence France Presse*, *Taliban Made \$400mn In 2011 From Taxes, Extortion: UN* (Sept. 11, 2012), <https://www.nation.co.ke/news/world/Taliban-made--400-mn/1068-1504748-w0sl0a/index.html>.

⁴⁴⁷ Praveen Swami, *Why Terrorists Aren’t Scared of Sanctions*, *The Hindu* (Sept. 12, 2012).

operating in Afghanistan. As part of those efforts, Defendants' standard practice would have been to conduct basic research on the Afghan market and the mechanics of local subcontracting. Even cursory research of that nature would have uncovered the press reports discussing protection payments set forth above, or other similar reports.

1093. Defendants' above-described knowledge applied equally to Defendants' "free goods" payments of cell phones to al-Qaeda and the Taliban, including its Haqqani Network. At all times, Defendants knew that al-Qaeda, the Taliban, and their allies prioritized obtaining U.S.-purchased cell phones for such phones' unique operational benefits to the terrorists.

1094. In the decades after 9/11, press reports regularly alerted Defendants to the Syndicate's desire to source U.S.-purchased phones to facilitate attacks against Americans in Afghanistan. On June 20, 2003, for example, the *Boston Globe* reported that al-Qaeda operative "Iyman Faris" "pleaded guilty to providing material support to terrorists and conspiracy to provide support" and admitted that he "attended an Al Qaeda training camp in Afghanistan," and, thereafter, "transported a cache of money and cellular phones for Al Qaeda" in "Afghanistan for use by bin Laden's fighters."⁴⁴⁸ A few months later, the *Associated Press* reported that "[p]rosecutors" stated that "Faris" "assisted al-Qaeda's work" when he "traveled to Pakistan and Afghanistan" and "carr[ie]d out low-level missions for [al-Qaeda] terrorists" by, among other things, "provid[ing]" "cell phones and cash to al-Qaeda members."⁴⁴⁹

⁴⁴⁸ Amber Mobley, *U.S. Citizen Admits Planning Al Qaeda Attack Trains and a Bridge Allegedly on Hit List*, *Boston Globe* (June 20, 2003), 2003 WLNR 3428108; see Derrill Holly, 20 years for alleged bridge plot;

⁴⁴⁹ Derrill Holly, *20 Years For Alleged Bridge Plot; Iyman Faris, 34, Tried to Withdraw a Guilty Plea; Prosecutors Say He Assisted Al-Qaeda's Work*, *Associated Press*, reprinted in *Philadelphia Inquirer* (October 29, 2003), 2003 WLNR 14764150.

1095. In later years, similar media reports documented al-Qaeda’s continuing efforts to source communications technologies, cell phones, and similar dual-use weapons from the United States. For example, on June 7, 2010, it was widely reported that a “federal grand jury” “charged a Texas man with attempting to provide al Qaeda with global positioning instruments, cell phones and a restricted publication on U.S. weapons in Afghanistan.”⁴⁵⁰

1096. Such reports also alerted Defendants that al-Qaeda’s and the Taliban’s reliance upon iconic American communications technologies deepened in the late 2000s, not unlike the knowledge, communications security, and communications efficiency benefits, among others, familiar to most smartphone users after the iPhone revolutionized the space in the late 2000s.

2. Defendants Knew That Their The U.S. Government Opposed Defendants’ Payment Of Protection Money To The Taliban, Including Its Haqqani Network

1097. The U.S. government did not approve, publicly or privately, of Defendants’ protection payments. The government relied on its chosen Western contractors – including Defendants – to take responsibility for ensuring the financial integrity of their contracting practices in Afghanistan. At all times, the government conveyed the message that protection payments violated U.S. law and undermined U.S. foreign-policy objectives in Afghanistan.

1098. The U.S. government has long been on record that protection payments to terrorists are unlawful – no matter their motivation. On March 19, 2007, Chiquita Brands International, Inc. (“Chiquita”), a multinational banana supplier, pleaded guilty in this District to having provided material support to the United Self-Defense Forces of Colombia (“AUC”) in

⁴⁵⁰ David C. Morrison, *Behind the Lines: Our Take on the Other Media’s Homeland Security Coverage*, CQ Homeland Security (June 7, 2010), 2010 WLNR 11991958.

Colombia.⁴⁵¹ Chiquita had routed protection payments to the AUC – then designated as a Specially Designated Global Terrorist – “through various intermediaries,” and had falsely accounted for them as “security payments.”⁴⁵² Chiquita later argued that it paid AUC protection money “under threat of violence,” but the U.S. Department of Justice responded that the “payments were illegal and could not continue.”⁴⁵³ It thus charged Chiquita with (and Chiquita pleaded to) the federal crime of transacting with a Specially Designated Global Terrorist.⁴⁵⁴

1099. In the public press release announcing the plea deal, an Assistant Attorney General stated: “Like any criminal enterprise, a terrorist organization needs a funding stream to support its operations. . . . Thanks to Chiquita’s cooperation and this prosecution, that funding stream is now dry and corporations are on notice that they cannot make protection payments to terrorists.”⁴⁵⁵ A U.S. Attorney further emphasized: “Funding a terrorist organization can never be treated as a cost of doing business. . . . American businesses must take note that payments to terrorists are of a whole different category. They are crimes.”⁴⁵⁶

1100. On information and belief, Defendants were aware of the *Chiquita* settlement and its clear message that the U.S. government considered protection payments illegal. The settlement received extensive scrutiny among the international business community and was the

⁴⁵¹ See Plea Agreement, *United States v. Chiquita Brands Int’l, Inc.*, No. 07-cr-00055-RCL (D.D.C. filed Mar. 19, 2007), Dkt. 11.

⁴⁵² Press Release, U.S. Dep’t of Justice, *Chiquita Brands International Pleads Guilty To Making Payments To A Designated Terrorist Organization & Agrees To Pay \$25 Million Fine* (Mar. 19, 2007) (“*Chiquita Brands International Pleads Guilty*”).

⁴⁵³ *Id.*

⁴⁵⁴ See 50 U.S.C. §§ 1701, 1705; 31 C.F.R. §§ 594.201(a), 594.701(c); Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001).

⁴⁵⁵ *Chiquita Brands International Pleads Guilty*.

⁴⁵⁶ *Id.*

subject of recurring media coverage. Media outlets describing the settlement included *United Press International* on March 14, 2007; the *Washington Times* on March 19, 2007; the *Associated Press* the next day; and the *Washington Post* on August 2, 2007.⁴⁵⁷

1101. The U.S. government viewed protection payments in Afghanistan the same way. Government officials stated that, as with Chiquita's payments to terrorists in Colombia, protection payments to the Taliban were unlawful and undermined U.S. reconstruction objectives. For example, at a House Subcommittee hearing, an Assistant Deputy Defense Undersecretary for Program Support was asked whether "facilitation payments . . . to provincial governors, to local police or warlords in order to ensure that trucks aren't bothered [are] legal under United States law?"⁴⁵⁸ He responded: "Clearly, it's not . . . and it's counterproductive to what we're trying to do."⁴⁵⁹ The U.S. Special Inspector General for Afghanistan Reconstruction ("SIGAR") similarly opined that "I don't think that there should ever be or ever condone paying off a Taliban entity for anything . . . Obviously that's wrong; it's against the law and counter to any counterinsurgency or reconstruction initiative that we would like to see put in place."⁴⁶⁰

1102. The congressional Commission on Wartime Contracting found it "particularly alarming" that "subcontractors on U.S.-funded convoys, road construction, and development

⁴⁵⁷ See United Press International, *Chiquita To Pay \$25M For Terrorist Payoffs* (Mar. 14, 2007); Matt Apuzzo, *Chiquita Pleads Guilty To Doing Business With Terrorists*, Assoc. Press (Mar. 20, 2007); *Chiquita Pleads To Protection Payoffs*, Wash. Times (Mar. 19, 2007); Carol D. Leonnig, *In Terrorism-Law Case, Chiquita Points to U.S.*, Wash. Post (Aug. 2, 2007).

⁴⁵⁸ *Hearing on Corruption in Afghanistan Defense Contracting* (statement by Rep. John F. Tierney (D. Mass.)).

⁴⁵⁹ *Id.* (statement of Assistant Deputy Undersecretary Gary Motsek).

⁴⁶⁰ *Funding The Enemy* at 196.

projects pay insurgent groups for protection.”⁴⁶¹ Based on such statements, Defendants knew that the U.S. government was institutionally opposed to protection-money payments.

1103. Protection payments also violated express U.S. government contracting requirements and regulations. Under the terms of their contracts, prime contractors bore responsibility for ensuring the integrity of U.S. spending in Afghanistan. The government further imposed requirements designed to ensure that private contractors lived up to that responsibility. For example, USAID’s contracts contained a “standard clause” reminding its contractors that “U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the contractor/recipient to ensure compliance with these Executive Orders and laws.”⁴⁶² U.S. Central Command (“CENTCOM”) contracts similarly were required to contain a standard clause requiring government contractors to comply with all U.S. and Afghan laws, which included a prohibition on providing material support to terrorists.⁴⁶³

1104. Prime contractors were required to include those same clauses in their contracts with – and ensure compliance by – their subcontractors.⁴⁶⁴ The “vetting” requirements were

⁴⁶¹ *CWC Report* at 73.

⁴⁶² Memorandum from Bruce N. Bower, USAID Regional Inspector General to Earl W. Gast, USAID Afghanistan Director, *Review Of Security Costs Charged To USAID’s Projects In Afghanistan* (Review Report No. 5-306-10-002-S) at 11 (Sept. 29, 2010) (“*2010 USAID OIG Report*”), <https://oig.usaid.gov/sites/default/files/2018-06/5-306-10-002-s.pdf>.

⁴⁶³ See Office of Under Secretary of Defense, *Class Deviation – Implementation Of The Synchronized Predeployment & Operational Tracker (SPOT) To Account For Contractor Personnel Performing In The United States Central Command Area Of Responsibility*, Memorandum for Directors Of Defense Agencies (Oct. 17, 2007).

⁴⁶⁴ See, e.g., USAID Contract No. DFD-I-00-05-00250, § H.15 (Sept. 27, 2005) (issued to Defendant DAI) (“[t]his provision must be included in all subcontracts/subawards”); USAID Contract No. 306-C-00-11-00506, § H.17 (Oct. 29, 2010) (issued to Defendant Black & Veatch Special Projects Corporation) (“[t]his provision must be included in all subcontracts/subawards”).

especially strict for any subcontractors that were to be armed under the contracts. Moreover, the Defense Contract Audit Agency's audit manual promulgated guidance instructing that "prime contractor oversight of subcontractors" should, among other things, "include technical and financial performance monitoring" and "ensure that payment to the subcontractor for the work accomplished was in accordance with the subcontract terms and based on allowability, allocability and reasonableness principles."⁴⁶⁵ Most Defendants' protection payments – whether made directly, or through subcontractors – violated those requirements and reflected a failure to live up to their responsibility to ensure the legality of their contract spending in Afghanistan.

1105. Contractors typically concealed their individual payments from the U.S. government by funneling the money through networks of subcontractors and mischaracterizing the payments in their books and records as "security" costs. For that reason, the U.S. government was unaware of the specific illegal payments that Defendants made.

1106. As the U.S. government became aware of broader patterns of protection payments in Afghanistan, it implemented a number of programs to curtail them. For example, it created the ATFC and Task Force 2010, both of which were interagency groups that drew on intelligence assets to identify and interrupt flows of contracting money to the insurgency. Congress also created SIGAR, which scrutinized and audited government contracting as part of a broader anti-corruption mandate. And USAID implemented several programs – including Accountable Assistance for Afghanistan – to "ensure the proper procedures are in place to help protect assistance dollars from being diverted from their development purpose by extortion or

⁴⁶⁵ SIGAR, *Progress Made Toward Increased Stability Under USAID's Afghanistan Stabilization Initiative-East Program But Transition To Long Term Development Efforts Not Yet Achieved* at 9, SIGAR Audit No. 12-11 (June 29, 2012).

corruption.”⁴⁶⁶ The net effect of these various efforts was to elevate anti-corruption to a distinct line of effort in the Coalition’s campaign plan, and to convey unmistakably to industry participants that protection payments were unacceptable.

1107. The U.S. government also implemented a broader array of programs designed to combat corruption in Afghanistan. Those programs, which included SIGAR audits and a variety of initiatives carried out under the auspices of Task Force Shafafiyat, reflected the U.S. policy imperative of reducing corruption throughout Afghanistan. That effort, led by then-Brigadier General H.R. McMaster, evinced a vigorous commitment by the U.S. military in 2009 and afterwards to stamp out corruption in Afghanistan. The outgoing ISAF Commander underscored the importance of those measures to U.S. policy: as he briefed President Obama in 2013, “corruption is the existential, strategic threat to Afghanistan.”⁴⁶⁷ Defendants’ payments fueled the type of corruption that U.S. agencies were attempting to eradicate.

1108. The U.S. government on occasion encouraged companies to hire local Afghans or employ local Afghan businesses in connection with some projects. This was not a license for Defendants to hire Taliban fighters or to allow their Afghan partners to pay insurgents. On the contrary: the U.S. government at all times communicated an expectation that Defendants should vet their local partners and take affirmative steps to ensure that the money they paid to those partners did not flow to the Taliban. And the U.S. government repeatedly made clear that the payment of protection money – or the payment of Taliban “taxes” – in exchange for permission to proceed with U.S.-funded projects was illegal and counterproductive. Neither USAID nor

⁴⁶⁶ USAID, *Fact Sheet On Accountable Assistance for Afghanistan* (June 2011).

⁴⁶⁷ Joint and Coalition Operational Analysis (JCOA), *Operationalizing Counter/Anti-Corruption Study* at 1 (Feb. 28, 2014) (emphasis in original), <https://www.hsd.org/?view&did=756004>.

ISAF ever suggested that such payments were either an inevitable consequence or an acceptable cost of implementing U.S.-funded projects in Taliban areas.

1109. In September 2010, General Petraeus issued formal contracting guidance designed to further discourage protection payments to the Taliban. In the guidance document, General Petraeus emphasized that “[w]here our money goes is as important as the service provided or the product delivered.”⁴⁶⁸ He thus instructed contracting officers to “[h]old prime contractors responsible for the behavior and performance of their sub-contractors,” with an understanding that “[e]xcessive sub-contracting tiers provide opportunities for criminal networks and insurgents to divert contract money from its intended purpose.”⁴⁶⁹ At bottom, the U.S. government’s goal was to improve its systems and ensure that its “vendors and contractors” did not “empower the wrong people or allow the diversion of funds” to insurgents.⁴⁷⁰ The government took a number of steps to implement that guidance, including by ramping up its vetting efforts and affirmatively suspending or debarring certain contractors with suspected links to insurgents.

1110. Defendants nonetheless remained able to execute their payments to insurgents despite the U.S. government’s efforts to stop them, for several reasons. *First*, the government often lacked visibility into the subcontracting networks through which the payments flowed and so had to “rely exclusively on prime contractors” to vet and supervise the subcontractors.⁴⁷¹ When Defendants knowingly (or recklessly) funneled protection money through those subcontractors, the structure of the transactions made it difficult for the government to trace the

⁴⁶⁸ *COMISAF’s Contracting Guidance* at 1.

⁴⁶⁹ *Id.*

⁴⁷⁰ *Id.*

⁴⁷¹ U.S. Special Inspector General for Afghanistan Reconstruction, *Contracting With The Enemy: DOD Has Limited Assurance That Contractors With Links To Enemy Groups Are Identified And Their Contracts Terminated* at 8, Audit No. 13-6 (Apr. 2013).

money with enough precision to take corrective action. Such payments frustrated the U.S. military's policy of identifying and terminating "contracts with supporters of the insurgency."⁴⁷²

1111. *Second*, the U.S. government faced staffing shortages that impeded its efforts to fully monitor the large number of contractors and subcontractors operating in Afghanistan. With a limited number of qualified contracting officers available – and a vast network of contracts to supervise – the government lacked the resources to investigate every payment made by Defendants or their subcontractors. Defendants were able to exploit those resource constraints to conceal their protection payments from U.S. government personnel, when they should have been the ones to flag such issues for the agencies funding their projects with U.S. taxpayer money.

1112. *Third*, the U.S. government relied on the good faith of its contractors to prevent payments to the insurgents, because the contractors often had access to better on-the-ground information than did the government. Due to Defendants' business ties – and the long in-country tenures of many of their personnel, as compared to the typically short rotations of U.S. government deployments – Defendants had unique real-time visibility into where their money was going. That made it even easier to conceal their payments from U.S. regulators.

1113. As one senior terror-finance investigator for the U.S. government explained in an interview with SIGAR, for a government investigator in Afghanistan:

[I]t takes 6-9 months to understand what's going on, become cognizant. You hit your stride at 12 to 15 months. It's that base of knowledge to know who, what, to follow threats, say oh this is a problem. To get access to records (for forensic accounting), you need demonstrated suspicious behavior.

Therefore *continuity* is critical. It was typically *contractors*, not government, who provided continuity – [Subject Matter Experts] who eat, live and breathe this stuff. In contrast, the military is assigned, but does not have specialization in these areas.⁴⁷³

⁴⁷² *Id.*

⁴⁷³ *SIGAR Interview with Gert Berthold* at 4 (emphasis in original).

Given those constraints, it was Defendants (not the U.S. government) that had the resources, expertise, and obligation to ensure that their practices did not materially support the Taliban.

1114. In sum, the U.S. government clearly stated its opposition to protection payments and attempted to curtail them. But those efforts were imperfect, and, at all times, Western contractors, including Defendants, functioned as the U.S. government's principal tool against terrorist financing. But Defendants abused that trust to pay off the Taliban and increase their profit margins. Defendants' conduct forms the basis of this lawsuit; Plaintiffs expressly disclaim any challenge to the U.S. government's policy decisions.

IX. DEFENDANTS' FINANCIAL, LOGISTICAL, AND OPERATIONAL ASSISTANCE TO THE IRGC AND PROTECTION PAYMENTS TO THE TALIBAN FLOWED THROUGH TO FACILITATE TERRORIST ATTACKS AGAINST AMERICANS IN AFGHANISTAN THAT WERE PLANNED, AUTHORIZED, AND SOMETIMES JOINTLY COMMITTED BY AL-QAEDA

A. In Furtherance Of The IRGC Conspiracy, The IRGC Relied Upon Defendants' Resources To Provide Key Assistance To Al-Qaeda And The Taliban, Including Its Haqqani Network, That Facilitated Terrorist Attacks Against Americans In Afghanistan In Order To Drive The United States Out Of Afghanistan In Furtherance Of The IRGC's Conspiracy

1115. Defendants provided the funds, technologies, services, and support necessary for the IRGC to sustain its decades-long, robust support for al-Qaeda and the Taliban, including its Haqqani Network, as they mutually sought, alongside the IRGC, to expel the United States from Afghanistan through a campaign of IRGC-sponsored terrorism in Afghanistan that was committed, planned, and authorized by al-Qaeda.

1116. The IRGC has long provided support – routed through Hezbollah and the Qods Force – for al-Qaeda-led terrorist attacks against American military forces and contractors in Afghanistan and Iraq. For example, Hezbollah, the Qods Force, and Regular IRGC sponsored a substantial training, logistics, travel, and communications campaign, all of which was

implemented by the IRGC in Lebanon, Iran, Iraq, and Afghanistan) using IRGC, including Hezbollah and the Qods Force, resources that enabled Hezbollah and the Qods Force to flow resources and training to al-Qaeda and Taliban, including Haqqani Network, terrorists who facilitated attacks against Americans in Afghanistan.

1117. The IRGC intentionally used Hezbollah and the Qods Force to lead every aspect of its support for al-Qaeda and Taliban attacks against Americans in Afghanistan, at least in part, because the IRGC wanted “plausible deniability” of Iranian involvement based upon the Iranian propaganda that Hezbollah is not and was not an Iranian agent. To that end, when ZTE and Huawei (alongside co-conspirator MTN) provided embargoed technology and funds, and any other materials useful for terrorist tradecraft to their IRGC front counterparties, those items flowed through such IRGC-related parties to Hezbollah and the Qods Force, which, in turn, distributed money, arms, and technology to the IRGC’s proxies in Afghanistan, al-Qaeda and the Taliban, including its Haqqani Network. In this way, the IRGC maintained influence on the Afghanistan Terror Campaign while simultaneously delegating its planning, commission, and authorization to al-Qaeda and the Haqqani Network, who were two of the IRGC’s key allies amongst the Syndicate.

1. The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support For Anti-American Terrorism In Afghanistan To Undermine The U.S. Mission There

1118. Although there are religious differences between the Shiite Iranian regime and the Sunni Taliban organization, those differences have not deterred the IRGC from supporting the Taliban’s terrorist activities. The IRGC and the Taliban share a core geopolitical aim: to inflict mass casualties on Americans in the region. As two military-intelligence scholars observed, “the Iranian regime is ideologically and religiously opposed to the Taliban, [but] it nevertheless views

the group as a useful counterweight to the United States.”⁴⁷⁴ Similarly, as a Taliban commander stated in 2010 of Iran, “Our religions and our histories are different, but our target is the same – we both want to kill Americans.”⁴⁷⁵ Sectarian distinctions aside, the IRGC has supported and funded attacks by the Taliban on U.S. and allied forces in Afghanistan to harm the United States.

1119. The Fourth Corps of the Qods Force, one of its four regional commands, implements Iran’s foreign policy in Afghanistan.⁴⁷⁶ During the relevant timeframe, the Qods Force did so largely by providing the Taliban (including the Haqqani Network) with material support for terrorist attacks in Afghanistan. The Fourth Corps’ al-Ansar Command Center is based in Iran’s second-largest city, Mashhad, near the border with Afghanistan.⁴⁷⁷ Mashhad naturally serves as a stopping point between Afghanistan and Tehran, Iran’s capital.⁴⁷⁸

1120. In the months after 9/11, the IRGC met with senior Taliban officials to offer military aid to support the Taliban’s fight against U.S.-led Coalition forces. The IRGC planned that meeting and hosted it on the Iranian side of the Afghanistan border. As part of this initial offer of support, the IRGC pledged to sell advanced military equipment to the Taliban for use against U.S. and allied forces, boasted of the IRGC’s ability to track U.S. troop movements, and promised to allow terrorists entering Afghanistan to travel through Iranian territory. The IRGC also provided safe harbor to Taliban leaders who escaped U.S. forces.

⁴⁷⁴ *Iran’s Balancing Act* at 5.

⁴⁷⁵ Bill Roggio, *Taliban Commander Linked To Al Qaeda, Iran, Killed In US Strike In Western Afghanistan*, Long War J. (July 16, 2010).

⁴⁷⁶ *JIEDDO Report* at 5.

⁴⁷⁷ Joseph Felter & Brian Fishman, *Iranian Strategy in Iraq, Politics and “Other Means”* at 18, Combating Terrorism Center (Oct. 13, 2008).

⁴⁷⁸ *JIEDDO Report* at 5.

1121. Immediately following the U.S. invasion of Afghanistan, the IRGC made a pretense of professing support for the U.S. and NATO mission, but in reality was already seeking to undermine it. In February 2002, then-CIA Director George J. Tenet testified before Congress that “initial signs of Tehran’s cooperation and common cause with us in Afghanistan are being eclipsed by Iranian efforts to undermine US influence there. While Iran’s officials express a shared interest in a stable government in Afghanistan, the IRGC appeared bent on countering the US presence.”⁴⁷⁹ As one scholar explained, the IRGC “feared the US might use Afghanistan as a base from which to launch a kinetic attack on Iran. The Taliban insurgency thus became viewed by Tehran as a tool with which to keep American forces preoccupied.”⁴⁸⁰

1122. The U.S. government documented the IRGC’s escalating support for the Taliban terrorists over the course of the United States’ involvement in Afghanistan. In April 2007, General Peter Pace, Chairman of the U.S. Joint Chiefs of Staff, stated that Iranian explosives had been captured in Kandahar Province en route to the Taliban but acknowledged that it was not yet entirely clear who within Iran was responsible.⁴⁸¹ The next day, U.S. Assistant Secretary of State Richard Boucher described “a series of indicators that Iran is maybe getting more involved in an unhealthy way in Afghanistan.”⁴⁸²

1123. Those indicators rapidly grew in intensity, and soon there was little doubt that the IRGC was actively sponsoring the Taliban terrorists as a core part of its foreign policy. A

⁴⁷⁹ *DCI Testimony: Converging Dangers in a Post 9/11 World*, Central Intelligence Agency (Feb. 6, 2002).

⁴⁸⁰ Farhad Rezaei, *Iran and the Taliban: A Tactical Alliance?*, The Begin-Sadat Center for Strategic Studies (Jan. 15, 2019) (“*Iran and the Taliban: A Tactical Alliance?*”).

⁴⁸¹ Breffni O’Rourke, *Afghanistan: U.S. Says Iranian-Made Weapons Found*, RadioFreeEurope (Apr. 18, 2007).

⁴⁸² *Id.*

purported May 2007 U.S. State Department cable (as published online), for example, reported that Afghan President Hamid Karzai had expressed concerns “over Iranian agents engaging Taliban and supplying them with weapons.” A purported July 2007 U.S. State Department cable (as published online) similarly reported that Taliban terrorists had received “light weapons and grenade launchers [that] bore the stamps of the Iranian factories where they were manufactured, primarily in 2006 and 2007.” The same cable explained that the fighters claimed they had received training in Iran and had been promised access to antiaircraft rockets by IRGC officials. A purported military-intelligence summary the next month (as published online), reported on an “‘alarmingly rapid increase’ in Iranian presence in Afghanistan.”

1124. When the U.S. Treasury Department designated the Qods Force as a SDGT later in 2007, it confirmed that the “Qods Force provides weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan.”⁴⁸³ As the designation explained:

The Qods Force is the Iranian regime’s primary instrument for providing lethal support to the Taliban. The Qods Force provides weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan. Since at least 2006, Iran has arranged frequent shipments of small arms and associated ammunition, rocket propelled grenades, mortar rounds, 107mm rockets, plastic explosives, and probably man-portable defense systems to the Taliban. . . . Through Qods Force material support to the Taliban, we believe Iran is seeking to inflict casualties on U.S. and NATO forces.⁴⁸⁴

1125. Similar observations continued in 2008. According to the U.S. State Department’s 2008 Country Reports on Terrorism: “The Qods Force, an elite branch of the Islamic Revolutionary Guard Corps (IRGC), is the regime’s primary mechanism for cultivating and supporting terrorists abroad. The Qods Force provided aid in the form of weapons, training,

⁴⁸³ Press Release, U.S. Treasury Dep’t, *Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007).

⁴⁸⁴ *Id.*

and funding to HAMAS and other Palestinian terrorist groups, Lebanese Hizballah, Iraq-based militants, and Taliban fighters in Afghanistan.”⁴⁸⁵

1126. The U.S. government’s Joint IED Defeat Organization (JIEDDO) recognized in a 2009 report that “Iran’s intentions are the same in both Afghanistan and Iraq: to develop, fund and arm proxy networks to leverage against the perceived U.S. aim of pursuing an active regime change doctrine in Iran.”⁴⁸⁶ Similarly, a purported January 2010 cable (as published online) explained that senior officials from the United Arab Emirates’ State Security Department had accused Iran, through the IRGC, of supporting the Taliban by providing money and weapons, smuggling drugs, and facilitating the movement of Taliban leaders and fighters.

1127. According to another purported February 2010 cable (as published by online), President Karzai’s Chief of Staff and former Ambassador to Iran, Omar Daudzai, reported that Iranian officials were no longer denying the IRGC’s support for the Taliban in Afghanistan, instead remaining silent in the face of the assertion by the Government of Afghanistan.

1128. By April 2010, the U.S. Department of Defense reported that the IRGC was “covertly” supporting the Taliban. “Arms caches have been recently uncovered with large amounts of Iranian manufactured weapons, to include 107mm rockets, which we assess IRGC-QF delivered to Afghan militants.”⁴⁸⁷ It further explained that “Tehran’s support to the Taliban is inconsistent with their historic enmity, but fits with Iran’s strategy of backing many groups to ensure that it will have a positive relationship with the eventual leaders.”⁴⁸⁸

⁴⁸⁵ U.S. State Dep’t, *Country Reports on Terrorism 2008* at 182-83 (Apr. 2009).

⁴⁸⁶ *JIEDDO Report* at 5.

⁴⁸⁷ Unclassified Report on Military Power of Iran (Apr. 2010), https://fas.org/man/eprint/dod_iran_2010.pdf.

⁴⁸⁸ *Id.*

1129. On August 3, 2010, the U.S. Treasury Department – pursuant to Executive Order 13224 – designated General Hossein Musavi and Colonel Hasan Mortezaei, senior officials in the Qods Force, as SDGTs for their roles in supporting the Taliban.⁴⁸⁹ General Musavi was the leader of the Ansar Corps, also known as the Fourth Corps, the branch of the Qods Force responsible for carrying out activities within Afghanistan.⁴⁹⁰ The U.S. Treasury Department found that both General Musavi and Colonel Mortezaei, acting in their capacity as senior Qods Force officers, had provided “financial and material support to the Taliban.”⁴⁹¹ The U.S. Treasury Department further concluded that “the IRGC-QF provides select members of the Taliban with weapons, funding, logistics and training.”⁴⁹²

1130. General David Petraeus, then the Commander of the ISAF, testified before the Senate Armed Services Committee in March 2011 that the IRGC “without question” supplied weapons, training, and funding to the Taliban in order to “make life difficult” for U.S. and NATO forces in Afghanistan.⁴⁹³

1131. When the U.S. Department of Defense provided Congress with its Annual Report on Military Power of Iran in April 2012, it explained that, even though Iranian “support to the Taliban is inconsistent with their historic enmity, it complements Iran’s strategy of backing many groups to maximize its influence while also undermining U.S. and [NATO] objectives by

⁴⁸⁹ Press Release, U.S. Treasury Dep’t, *Fact Sheet: U.S. Treasury Department Targets Iran’s Support for Terrorism Treasury Announces New Sanctions Against Iran’s Islamic Revolutionary Guard Corps-Qods Force Leadership* (Aug. 3, 2010).

⁴⁹⁰ *Id.*

⁴⁹¹ *Id.*

⁴⁹² *Id.*

⁴⁹³ *The Situation in Afghanistan: Hr’g Before the S. Comm. On Armed Services*, 112 Cong. 40 (Mar. 15, 2011) (statement of General David Petraeus), <https://www.govinfo.gov/content/pkg/CHRG-112shrg72295/pdf/CHRG-112shrg72295.pdf>.

fomenting violence.”⁴⁹⁴ By means of “the IRGC-QF, Iran provides material support to terrorist or militant groups such as . . . the Taliban.”⁴⁹⁵ The U.S. Department of Defense characterized the support as part of a “grand strategy” to “challeng[e] U.S. influence.”⁴⁹⁶

1132. In its 2012 Report on Progress Toward Security and Stability in Afghanistan, the U.S. Department of Defense reported to Congress that the IRGC was engaging in “covert activities” in Afghanistan, including the provision of weapons and training to the Taliban.⁴⁹⁷ As the report explained, “Since 2007, Coalition and Afghan forces have interdicted several shipments of Iranian weapons. Tehran’s relationship with the insurgency, although not ideologically based, is consistent with Iran’s short- to mid-term goal of undermining Coalition efforts and opposing the international military presence in Afghanistan.”⁴⁹⁸

1133. Less than two years later, the U.S. Treasury Department concluded that the Qods Force “utilized now-detained Afghan associate, Sayyed Kamal Musavi, who was designated today, to plan and execute attacks in Afghanistan.” It further confirmed that “[t]wo IRGC-QF officers also designated today, Alireza Hemmati and Akbar Seyed Alhosseini, provided logistical support to this associate.”⁴⁹⁹ Similarly, according to a Taliban commander in central Afghanistan in 2015: “Iran supplies us with whatever we need.”⁵⁰⁰

⁴⁹⁴ *Annual Report on Military Power of Iran 2* (Apr. 2012).

⁴⁹⁵ *Id.* at 3.

⁴⁹⁶ *Id.* at 1.

⁴⁹⁷ U.S. Dep’t of Def., *Report on Progress Toward Security and Stability in Afghanistan* at 148 (Dec. 2012).

⁴⁹⁸ *Id.*

⁴⁹⁹ Press Release, U.S. Treasury Dep’t, *Treasury Targets Networks Linked To Iran* (Feb. 6, 2014).

⁵⁰⁰ Margherita Stancati, *Iran Backs Taliban With Cash And Arms*, Wall St. J. (June 11, 2015).

1134. In 2016, Taliban leader Mullah Mansour was killed by an American drone strike while returning to Afghanistan from Tehran, where he had been meeting with Iranian security officials, and possibly directly with Ayatollah Ali Khameni, to discuss tactical coordination of Taliban terrorist activities in Afghanistan. He had made at least two visits to Iran since 2013.

1135. The IRGC's support for terrorist groups in Afghanistan has continued. The U.S. State Department stated in 2017 that "Iran is responsible for intensifying multiple conflicts and undermining the legitimate governments of, and U.S. interests in, Afghanistan" ⁵⁰¹ The U.S. Department of Defense similarly confirmed that the IRGC "provides some support to the Taliban and Haqqani Network." ⁵⁰² In May 2018, U.S. Secretary of State Michael Pompeo publicly accused the IRGC of supporting the Taliban and other terrorist groups in Afghanistan. ⁵⁰³

1136. In October 2018, the U.S. Treasury Department, pursuant to Executive Order 13224, designated additional Qods Force officials "for acting for or on behalf of IRGC-QF and for assisting in, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, the Taliban." ⁵⁰⁴ The U.S. Treasury Department acted along with the six other member nations of the Terrorist Financing Targeting Center – a multinational, cooperative effort to combat terrorism in the Middle East. ⁵⁰⁵

⁵⁰¹ *Country Reports on Terrorism 2017* at Foreword.

⁵⁰² U.S. Dep't of Def., *Enhancing Security and Stability in Afghanistan at 21* (June 2017).

⁵⁰³ *Mike Pompeo speech: What are the 12 demands given to Iran?*, Al Jazeera News (May 21, 2018).

⁵⁰⁴ Press Release, U.S. Treasury Dep't, *Treasury and the Terrorist Financing Targeting Center Partners Sanction Taliban Facilitators and their Iranian Supporters* (Oct. 23, 2018).

⁵⁰⁵ *Mike Pompeo speech: What are the 12 demands given to Iran?*, Al Jazeera News (May 21, 2018); Press Release, U.S. Treasury Dep't, *U.S. and Saudi Arabia to Co-Chair New Terrorist Financing Targeting Center* (May 1, 2017).

1137. The Secretary of Iran’s Supreme National Security Council, Ali Shamkhani, publicly acknowledged the IRGC’s support for the Taliban in January 2019, claiming that it was designed to “curb the security problems in Afghanistan.”⁵⁰⁶

1138. Most recently, the United States has recognized the IRGC’s support of the Taliban in the aftermath of Qassem Soleimani’s death. In a press conference in the days after the killing of General Soleimani, Secretary of State Michael Pompeo publicly accused the IRGC of backing the Taliban and associated groups, including the Haqqani Network.

1139. The IRGC, in turn, signaled its continued focus on destabilizing U.S. forces in Afghanistan by appointing General Esmail Ghaani (“Ghaani” or “Qaani”), the former head of the IRGC’s Qods Force branch in Afghanistan, to be the top commander of the Qods Force. General Ghaani traveled to Afghanistan in 2018 as the deputy ambassador of Iran to Kabul and remains focused on cultivating the IRGC’s relationship with the Taliban in Afghanistan.

1140. The Taliban’s reaction to Soleimani’s death similarly recognized the IRGC’s support for its terrorist activities. A Taliban statement condemned American forces for the attack on Soleimani and expressed regret for his “martyrdom.” Additional details were reported in Taliban-aligned publications about Soleimani’s support for the Taliban, including his meeting with Taliban delegations in Iran, personally traveling to Afghanistan, and planning attacks.

1141. Consistent with the policy described above, the IRGC provided material support or resources for the acts of extrajudicial killing that killed or injured Plaintiffs or their family members. As explained below, that support took the form of “currency . . . lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications

⁵⁰⁶ *Iran and the Taliban: A Tactical Alliance?*

equipment, facilities, weapons, lethal substances, explosives, personnel, . . . and transportation.”⁵⁰⁷

2. The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban, Including its Haqqani Network, With Weapons, Explosives, And Lethal Substances

1142. The IRGC provided material support or resources for the acts of extrajudicial killing that killed or injured Plaintiffs, or their family members, by providing (among other things) weapons, explosives, and lethal substances to the Taliban. Many of the weapons the IRGC provided were designed to be particularly effective against U.S. and allied forces operating in Afghanistan. For example, the IRGC provided the Taliban with anti-tank mines, long range rockets, explosively formed penetrators, suicide vehicle-borne improvised explosive devices, rocket-propelled grenades, and explosives, which were uniquely suited for terrorist attacks on U.S. and allied forces.

1143. U.S. and allied forces have seized large caches of IRGC-made weapons and explosives in Afghanistan, many of which bore markings of Iranian origin. A purported April 2007 military-intelligence summary (as published online) reported that “Iranian officials” were sending “to Afghanistan explosive devices and vehicles ready to be used as SVBIEDs [suicide vehicle-borne improvised explosive devices].”⁵⁰⁸ A purported U.S. government document from August of that year (as published online) also reported that the Afghanistan National Police had

⁵⁰⁷ 18 U.S.C. § 2339A(b)(1).

⁵⁰⁸ *Afghanistan War Logs: Anti-aircraft Missiles Clandestinely Transported From Iran Into Afghanistan – US Report*, The Guardian (July 25, 2010) (“*Anti-aircraft Missiles Clandestinely Transported*”); see also *Afghanistan War Logs: Afghan Government Seeking to Maintain Friendly Relations With Iran*, The Guardian (July 25, 2010) (referencing Iranian-made weapons recently found in Kandahar Province).

found evidence of a planning meeting for 25 suicide attacks in which it was stated that “[t]he materials for the bombs will be supplied by Iran Government”

1144. When the U.S. Treasury Department designated the Qods Force as a SDGT under Executive Order 13224 in October 2007, it specifically documented the IRGC’s frequent shipments of weapons to the Taliban over at least the prior year. A purported December 2007 military-intelligence summary (as published online) further reported that explosive samples in suicide vests seized from four suicide bombers “tasked by Taliban/Al-Qaeda leaders” with carrying out a suicide attack in Helmand Province were found to be a 92% probability of a match against a suspected sample of IRGC-sourced C4.

1145. In January 2008, a raid by Afghan Police in Farah Province discovered 130 mines, of which the Afghan Police concluded 60 were Iran-made.⁵⁰⁹ That same month the U.S. Ambassador to Afghanistan stated that “[t]here is no question that elements of insurgency have received weapons from Iran.”⁵¹⁰

1146. A purported June 2008 U.S. State Department cable (as published online) detailed multiple instances of the IRGC transferring arms to the Taliban in 2007 and 2008 and concluded that analyses of the weaponry “indicate the Taliban had access to Iranian weaponry produced as recently as 2006 and 2007.” Similarly, Afghan forces discovered a large cache of IRGC-made explosives hidden near the Bakhshabad Dam in Farah Province in March 2009. That same month, a purported military-intelligence summary (as published online) indicated that Taliban commanders had obtained portable surface-to-air missiles that originated in Iran.

⁵⁰⁹ *JIEDDO Report* at 10.

⁵¹⁰ Brian Bennett, *Iran Raises the Heat in Afghanistan*, *Time* (Feb. 22, 2008).

1147. In May 2009, 44 bricks of Iran-made explosives and dozens of Iran-made mortars were discovered in a Taliban stronghold in Helmand Province. Also in May 2009, Afghanistan border police intercepted a shipment crossing the Iranian border with dozens of anti-tank mines bound for Afghan militants. And in September 2009, a purported military-intelligence summary report (as published online) claimed that the Taliban had received “six very powerful anti-tank mines from Iran” to target ISAF forces or important Afghan Police Officers. That same year, the U.S. State Department reported that, “[s]ince at least 2006, Iran has arranged arms shipments to select Taliban members, including small arms and associated ammunition, rocket-propelled grenades, mortar rounds, 107mm rockets, and plastic explosives.”⁵¹¹

1148. By 2011, Taliban terrorists were using Iran-made and -sourced long-range rockets to attack Coalition targets in Afghanistan. In February 2011, British forces intercepted more than four dozen 122-milimeter rockets in Nimruz Province near the Iranian border, which gave the terrorists roughly double the range to attack Coalition targets. British Foreign Secretary William Hague stated that “detailed technical analysis, together with the circumstances of the seizure, leave us in no doubt that the weaponry recovered came from Iran.”⁵¹² The *Wall Street Journal* similarly reported that U.S. officials “said the rockets’ markings, and the location of their discovery, give them a ‘high degree’ of confidence that they came from the Revolutionary Guard’s overseas unit, the Qods Force.”⁵¹³ General Petraeus later confirmed that the Qods Force

⁵¹¹ U.S. State Dep’t, *Country Reports on Terrorism 2009* at 192 (Aug. 2010).

⁵¹² Julian Borger & Richard Norton-Taylor, *British Special Forces Seize Iranian Rockets In Afghanistan*, The Guardian (Mar. 9, 2011).

⁵¹³ Jay Solomon, *Iran Funnels New Weapons to Afghanistan and Iraq*, Wall St. J. (July 2, 2011).

had supplied these rockets to a “known Taliban facilitator.”⁵¹⁴ The U.S. Department of Defense’s 2011 Report on Progress Toward Security and Stability in Afghanistan similarly stated that “[f]orensics teams examined the rockets and confirmed an Iranian point of origin.”⁵¹⁵

1149. In June 2015, the IRGC hired smugglers to ferry supplies across the Iranian border and deliver them to Taliban units in Afghanistan. These IRGC-supplied weapons included 82mm mortars, light machine guns, AK-47 rifles, rocket-propelled grenades, and materials for making roadside bombs.

1150. The IRGC also provided the Taliban with rockets and similar weapons that were particularly effective against U.S. and Coalition forces. A purported April 2007 military-intelligence summary (as published online), for example, reported that the IRGC had purchased anti-aircraft missiles from Algeria in late 2006 and then smuggled them from Mashhad, Iran – where the Fourth Corps of the Qods Force is headquartered – into Afghanistan.⁵¹⁶ A purported Afghanistan Police Report from the next month (as published online) claimed that Iran intelligence sources issued three anti-aircraft launchers and ammunition to a Taliban commander. A purported march 2009 military intelligence summary (as published online) included intelligence reports of portable surface-to-air missiles arriving in Afghanistan from Iran. Similarly, a purported July 2009 military-intelligence summary (as published online) included reports of two dozen “Stinger” style surface-to-air missiles smuggled from Iran into Afghanistan.

⁵¹⁴ *The Situation in Afghanistan: Hr’g Before the S. Comm. On Armed Services*, 112 Cong. 40 (Mar. 15, 2011) (statement of General David Petraeus), <https://www.govinfo.gov/content/pkg/CHRG-112shrg72295/pdf/CHRG-112shrg72295.pdf>.

⁵¹⁵ U.S. Dep’t of Def., *Report on Progress Toward Security and Stability in Afghanistan* at 107 (Apr. 2011).

⁵¹⁶ *Anti-aircraft Missiles Clandestinely Transported*.

1151. According to a purported September 2009 military-intelligence summary (as published online), Taliban terrorists used an Iran-made rocket-propelled grenade launcher to shoot down Coalition helicopters. The launcher was marked “Made In Iran.” The launcher was particularly effective because, unlike some other launchers, the Iran-made launcher had a scope that could be adjusted for targeting and was more accurate for shooting helicopters.

3. The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Lodging, Training, Expert Advice Or Assistance, Safehouses, Personnel, And Transportation

1152. The IRGC also provided members of the Taliban and affiliated terrorist groups with lodging, training, expert advice or assistance, safe harbor, and transportation. The IRGC taught the Taliban attack techniques that were particularly effective against U.S. and Coalition forces. Without the training from the IRGC and its agents, the Taliban would not have been able to launch as successful a terrorist campaign against American forces.

1153. According to a purported June 2006 military-intelligence summary (as published online), two members of the Iranian Intelligence Secret Service had arrived in Parwan Province to help Taliban members “in carrying out terrorist attacks against the [Afghanistan] governmental authorities and the [Coalition] members, especially against the Americans forces.”⁵¹⁷ A purported military-intelligence summary later that year (as published online), reported that injured Taliban terrorists were evacuating to Tehran for shelter.⁵¹⁸

1154. The IRGC also trained Taliban fighters at camps within Iran. For example, a purported April 2007 military intelligence summary (as published online) reported that “Iranian

⁵¹⁷ *Afghanistan War Logs: US Claims Iran Spies Helping Insurgents to Attack Coalition Forces*, The Guardian (July 25, 2010).

⁵¹⁸ *Afghanistan War Logs: Iranians Alleged to Be Sheltering Wounded Taliban Fighters in Tehran*, The Guardian (July 25, 2010).

officials train” members of the Taliban at an Iranian base in Birjand, Iran, near the Afghanistan border.⁵¹⁹ A similar purported June 2007 military intelligence summary (as published online) claimed that the IRGC was training roughly 300 foreign fighters in Iran, presumably to fight in Afghanistan.

1155. A purported military-intelligence summary (as published online) from May 2008 claimed that a Taliban commander had traveled to Iran for training and returned with 40 trained terrorists. Similarly, a military-intelligence summary (as published online) from July 2008 referenced “trained fighters moving in from Iran.” And a purported military-intelligence summary (as published online) from October 2009 likewise reported on the return of a Taliban commander from training “in an Iran army barracks.”

1156. The IRGC provided Taliban terrorists with specialized training on how best to deploy IRGC-supplied weapons against U.S. and Coalition forces. A purported December 2008 military-intelligence summary (as published online) reported on a group of 40 insurgents “who allegedly were trained in an Iranian Military base” who had plans to attack the capital of Farah Province using weapons that “Iran Intelligence could have provided.” According to a purported April 2009 military-intelligence summary (as published online), the IRGC was recruiting Taliban terrorists for training in Iran on shooting down Coalition helicopters. And another purported April 2009 military-intelligence summary (as published online), reported on the return of a Taliban commander after receiving IED-manufacturing training in Iran.

1157. A March 21, 2010 article in London’s *The Sunday Times* reported extensively on Iranian security officials training Taliban recruits to “ambush” Coalition forces, attack checkpoints, and use guns and IEDs. The *Times* interviewed two Taliban commanders – from

⁵¹⁹ *Anti-aircraft Missiles Clandestinely Transported*.

Wardak and Ghanzi province – who had traveled to Iran with groups of Taliban terrorists for training, which improved their ability to launch lethal attacks on Coalition forces. According to the commanders, the IRGC paid for this travel and training. One commander who received training in Iran observed that the Taliban’s and Iran’s “religions and . . . histories are different, but our target is the same — we both want to kill Americans.”⁵²⁰

1158. By 2009, U.S government officials were openly accusing the IRGC of training the Taliban. In an August 2009 report, ISAF Commander General Stanley McChrystal explained that “the Iranian Qods Force is reportedly training fighters for certain Taliban groups and providing other forms of military assistance to insurgents.”⁵²¹ He confirmed again in May 2010 that the IRGC was training Afghan fighters in Iran.⁵²² In its 2009 Country Reports on Terrorism, the U.S. State Department reported: “Iran’s Qods Force provided training to the Taliban in Afghanistan on small unit tactics, small arms, explosives, and indirect fire weapons”⁵²³ Similarly, in 2012 it explained: “the IRGC-QF trained Taliban elements on small unit tactics, small arms, explosives, and indirect fire weapons, such as mortars, artillery, and rockets.”⁵²⁴

1159. The IRGC’s training of Taliban terrorists has not diminished. By 2015, the IRGC was operating at least four Taliban training camps within Iran.

1160. The IRGC also facilitated the Taliban’s attacks by allowing the Taliban to establish offices in Iran to serve as bases for planning terrorist attacks. For example, the IRGC

⁵²⁰ Miles Amoores, *Iranian military teaches Taliban fighters the art of ambush*, The Times (Mar. 21, 2010).

⁵²¹ Quoted by Sajjan M. Gohel, in *Iran’s Ambiguous Role in Afghanistan* at 13, CTC Sentinel (March 2010).

⁵²² *Killing Americans and Their Allies*.

⁵²³ U.S. State Dep’t, *Country Reports on Terrorism 2009* at 192 (Aug. 2010).

⁵²⁴ U.S. State Dep’t, *Country Reports on Terrorism 2012* at 196 (May 2013).

permitted a senior leader of the Taliban to set up an office in Zahedan, Iran, near the borders with Afghanistan and Pakistan. In or about 2014, the Taliban also opened an office in Mashhad, Iran, where the Fourth Corps of the Qods Force is headquartered.⁵²⁵ As of January 2019, the Taliban maintained an office in Tehran, Iran.⁵²⁶

1161. Hezbollah and Qods Force terrorists also conducted attacks alongside Taliban terrorists. In an October 2016 Taliban attack in Farah Province, four senior Qods Force commandos were killed, and many of the other Taliban dead were taken across the border to Iran for burial.

1162. Mohammad Arif Shahjahan, the governor of Farah Province in western Afghanistan, told Radio Free Afghanistan in 2017 that Taliban leaders had been traveling frequently to Iran, where they received protection and support.⁵²⁷ He reported that Qods Force operatives had recently met with and advised the Taliban in Farah Province.⁵²⁸

1163. The IRGC's training of Taliban terrorists in small unit tactics, small arms, explosives, indirect fire, and other techniques enabled the Taliban to more effectively attack U.S. forces and Coalition forces. The Taliban and affiliated terrorist groups in Afghanistan used the IRGC's training to kill or injure Plaintiffs or their family members.

⁵²⁵ Oved Lobel, *Afghanistan: The Forgotten Front Against Iran*, Australia/Israel & Jewish Affairs Council (Nov. 16, 2018).

⁵²⁶ *Iran and the Taliban: A Tactical Alliance?*

⁵²⁷ Abubakar Siddique & Noorullah Shayan, *Mounting Afghan Ire Over Iran's Support For Taliban*, Gandhara (July 31, 2017).

⁵²⁸ *Id.*

4. The IRGC, Including Its Hezbollah Division And Qods Force, Provided The Taliban With Financial Support

1164. The IRGC has also supported the Taliban financially. On an annual basis, the IRGC provided large cash payments to the Taliban. For example, a purported February 2005 military intelligence summary (as published online) reported that the IRGC delivered 10 million Afghanis (worth roughly \$212,000) to a location on Iran's border where the money was transferred to four members of a Taliban-associated terrorist group.⁵²⁹

1165. The IRGC also directly paid Taliban insurgents to kill U.S. forces. Another purported February 2005 military-intelligence summary (as published online) reported on a Taliban group that was being paid by the Iranian government \$1,740 for each Afghanistan soldier killed and \$3,481 for each Government of Afghanistan official killed. The report further explained that the group would begin attacking U.S. forces if the attacks on Afghans were successful.⁵³⁰ The IRGC paid Taliban terrorists an estimated \$1,000 for each U.S. soldier murdered in Afghanistan and \$6,000 for each destroyed American military vehicle. In one specific example, Taliban fighters received \$18,000 from the IRGC as a reward for an attack in 2010 that killed several Afghan forces and destroyed an American armored vehicle.⁵³¹

1166. The IRGC also provided funding to individual Taliban commanders, often as they were returning to Afghanistan from training in Iran. A purported May 2008 military-intelligence summary (as published online) reported on a Taliban leader returning from training in Iran "along with a considerable amount of money." A purported May 2009 U.S. State Department

⁵²⁹ *Afghanistan War Logs: Iran Smuggles Money into Afghanistan to Fund Insurgents, says US Report*, The Guardian (July 25, 2010).

⁵³⁰ *Afghanistan War Logs: Iran Offers Reward for Each Afghan Official and Soldier Killed, According to Coalition Report*, The Guardian (July 25, 2010).

⁵³¹ Miles Amoores, *Iran pays the Taliban to Kill US Soldiers*, The Times (Sept. 5, 2010).

Cable (as published online) stated that the IRGC may provide Taliban Commander Mullah Sangin with financial support to engage Coalition forces, including U.S. contractors.

1167. The IRGC has also supported the Taliban's finances by supporting its ability to traffic narcotics, which Taliban terrorists use "to finance their acts of terror and violence."⁵³² As the U.S. Treasury Department explained when it designated Iranian Qods Force General Gholamreza Baghbani as a Specially Designated Narcotics Trafficker in March 2012, General Baghbani allowed Afghan narcotics traffickers to smuggle opiates through the IRGC, facilitated the smuggling of chemicals necessary to produce heroin from Iran into Afghanistan, and helped "facilitate shipments of opium into Iran."⁵³³ General Baghbani also had narcotics traffickers deliver weapons on his behalf to the Taliban.⁵³⁴

1168. As reported in a 2015 *Wall Street Journal* article, a Taliban commander described the IRGC's financial support of the Taliban in the form of recruiting and paying individual terrorists. The commander explained that he had been detained for working illegally in Iran when he was approached by the IRGC and offered double his previous salary – to be paid by the IRGC – if he fought with the Taliban in Afghanistan.⁵³⁵ And in 2017, officials in Ghor Province accused the IRGC of financing a Taliban offensive that briefly enabled the Taliban to overtake a key district.⁵³⁶

⁵³² Press Release, U.S. Treasury Dep't, *Treasury Targets Taliban Shadow Governor of Helmand Afghanistan as Narcotics Trafficker* (Nov. 15, 2012).

⁵³³ Press Release, U.S. Treasury Dep't, *Treasury Designates Iranian Qods Force General Overseeing Afghan Heroin Trafficking Through Iran* (Mar. 7, 2012).

⁵³⁴ *Id.*

⁵³⁵ Margherita Stancati, *Iran Backs Taliban With Cash And Arms*, Wall St. J. (June 11, 2015).

⁵³⁶ Abubakar Siddique & Noorullah Shayan, *Mounting Afghan Ire Over Iran's Support For Taliban*, Gandhara (July 31, 2017).

5. The IRGC, Including Its Hezbollah Division And Qods Force, Provided Material Support to Al-Qaeda to Facilitate Syndicate Attacks in Afghanistan

1169. The IRGC has supported al-Qaeda's terrorist activities since the early 1990s, when Osama bin Laden lived in Sudan. The IRGC, Hezbollah, served as the original trainer for al-Qaeda with respect to suicide bombings, attacks against large buildings, IEDs, explosives, intelligence, and general attack tactics directed at American interests. For example, senior al-Qaeda operatives traveled to Iran and Lebanon during this period to camps run by Hezbollah and sponsored by the Qods Force.⁵³⁷ The operatives received advanced explosives training that enabled al-Qaeda to launch large-scale terrorist attacks on American embassies in Africa.⁵³⁸ According to one senior al-Qaeda official, trainers at this time were already researching how to develop shaped charges to pierce armor plating – the technology later perfected in EFPs.

1170. After 9/11, senior al-Qaeda leadership, sheltering in Iran under the patronage and with the counsel of Qods Force operatives, explicitly modeled their post-9/11 organization and tactics on the approach of Hezbollah and the Qods Force.

1171. While al-Qaeda was re-building itself in Iran after 9/11, the Iranians were busy rejecting U.S. and allied requests to stop aiding al-Qaeda. For example, on or about 2002 or 2003, Iran rejected a lawfully issued extradition request by the Jordanian government for Zarqawi on the preposterous grounds that Zarqawi – whom the Iranians knew well – was not Jordanian but, rather, Syrian. Similarly, in a 2003 face-to-face meeting in Geneva, Switzerland, then-U.S. ambassador to Iraq Ryan Crocker implored Iranian officials to cease their support for al-Qaeda's terrorism

⁵³⁷ *Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 151 (D.D.C. 2011) (“Prior to al Qaeda members’ training in Iran and Lebanon, al Qaeda had not carried out any successful large scale bombings.”).

⁵³⁸ *Id.*

targeting Americans in the Persian Gulf, which request the Iranians refused. By then, al-Qaeda had demonstrated its usefulness to the IRGC with respect to its ability to kill Americans, and the IRGC was already sheltering and supporting al-Qaeda's military leader, Saif al-Adel (who was also al-Qaeda's manager for Zarqawi's activities in Iraq) in his Qods Force-provided Tehran safehouse.

1172. The Iranians rebuffed U.S. outreach because the IRGC had already reached a secret deal with al-Qaeda. Following the 9/11 attacks on the United States and subsequent routing of Sunni terrorists in Afghanistan (including al-Qaeda) in late 2001, the IRGC met with senior al-Qaeda leaders who had fled Afghanistan into Iran to offer military aid to support al-Qaeda's fight against America. The IRGC hosted these meetings for its al-Qaeda "guests" throughout 2001 and 2002. As part of this initial offer of support, the IRGC pledged to provide funds and logistical support to facilitate the development of terrorist activities targeting Americans in countries bordering Iran. While the focus at the time was on Afghanistan, all involved expected the U.S. to eventually move into Iraq and for their shared terrorist enterprise to follow us there.

1173. Under this secret deal between the IRGC and al-Qaeda after 9/11, the IRGC intensified its material support for al-Qaeda's terrorist campaign against Americans around the world. Through the secret deal between the IRGC and al-Qaeda and the assistance that the former provided to the latter thereafter, the IRGC was the proximate and but-for cause of al-Qaeda's survival as a terrorist organization after 9/11 and the al-Qaeda linked terrorist attacks against Americans in Afghanistan, including Plaintiffs, that inevitably followed.

1174. Osama bin Laden personally concluded that al-Qaeda would have collapsed after 2001 without the secret deal and the IRGC's key support for al-Qaeda in the years following 9/11, and al-Qaeda's subsequent ability to execute terrorist attacks depended upon the "artery" provided

by the IRGC. For example, in 2007, bin Laden criticized an al-Qaeda terrorist who had been planning to strike IRGC-linked targets; in a secret internal al-Qaeda communique authored by bin Laden himself, bin Laden identified the key, organization-saving assistance that the IRGC had been providing to al-Qaeda after 9/11, stating because of the IRGC's historical support for al-Qaeda's terrorist operations, Iran was al-Qaeda's "*main artery for funds, personnel, and communication*."⁵³⁹

1175. Zawahiri also emphasized close strategic cooperation between al-Qaeda and the IRGC, following a pragmatic approach under which al-Qaeda focused on expanding its presence in Iran. Like bin Laden, Zawahiri agreed that al-Qaeda could not survive and thrive without the support it received from the IRGC. In a letter reportedly written by Zawahiri, al-Qaeda thanked the IRGC for the Qods Force's support in setting up al-Qaeda's terrorist network in Yemen in 2008 and stated, in effect, that al-Qaeda could not have established its franchise in Yemen without the IRGC's assistance.

1176. The U.S. government has also recognized the close partnership between the IRGC and al-Qaeda after the secret deal between the two. In July 2011, the U.S. Treasury Department designated as SDGTs six members of al-Qaeda operating in Iran under the previously described secret agreement between the IRGC and al-Qaeda.⁵⁴⁰ In so doing, the Treasury Department concluded that the secret deal provided that al-Qaeda terrorists "must refrain from conducting any operations within Iranian territory and recruiting operatives inside Iran while keeping Iranian

⁵³⁹ October 18, 2007 translated letter from Osama bin Laden to Karim at 1, *Bin Laden's Bookshelf*, Office of the Director of National Intelligence (2016) (emphasis added). In March 2016, the Office of the Director of National Intelligence declassified items that had been obtained by U.S. special operators in the May 2011 raid on bin Laden's compound, including this letter. See Bin Laden's Bookshelf, Office of the Director of National Intelligence.

⁵⁴⁰ Press Release, U.S. Treasury Dep't, *Treasury Targets Al-Qa'ida Funding and Support Network Using Iran as a Critical Transit Point* (July 28, 2011).

authorities informed of their activities. In return, the Government of Iran gave the Iran-based al-Qa'ida network freedom of operation and uninhibited ability to travel for extremists and their families” and permitted al-Qaeda to use Iran as a “critical transit point for funding to support [al-Qaeda’s] activities.” The Treasury Department also found that “Iran’s secret deal with al-Qa’ida” facilitated a terrorist network that “serves as the core pipeline through which al-Qa’ida moves money, facilitators and operatives from across the Middle East to South Asia.”⁵⁴¹ Indeed, al-Qaeda has honored its commitment to the IRGC despite its attacks on Shiite Muslims elsewhere in the Middle East.

1177. The U.S. Treasury Department has repeatedly recognized the link between al-Qaeda and the IRGC in making SDGT designations under Executive Order 13224. In February 2012, the agency designated the Iranian Ministry of Intelligence and Security (“MOIS”) as a terrorist-sponsoring entity for, among other things, supporting al-Qaeda.⁵⁴² In 2014, the agency likewise designated a “key Iran-based” al-Qaeda facilitator who has “assisted extremists and operatives transiting Iran on their way into and out of Pakistan and Afghanistan.”⁵⁴³

1178. The close relationship between al-Qaeda and the IRGC has continued in recent years. In 2017, the U.S. State Department explained, “Since at least 2009, Iran has allowed [al-Qaeda] facilitators to operate a core facilitation pipeline through the country, enabling [al-Qaeda] to move funds and fighters to South Asia and Syria.”⁵⁴⁴ It further accused the IRGC of remaining

⁵⁴¹ *Id.*

⁵⁴² Press Release, U.S. Treasury Dep’t, *Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism* (Feb. 16, 2012).

⁵⁴³ Press Release, U.S. Treasury Dep’t, *Treasury Targets Networks Linked To Iran* (Feb. 6, 2014).

⁵⁴⁴ U.S. State Dep’t, *Country Reports on Terrorism 2016* at Iran Section (July 2017).

unwilling to bring to justice or identify al-Qaeda members in its custody.⁵⁴⁵ The next year, the agency reaffirmed those conclusions and reiterated the IRGC's close relationship with al-Qaeda.⁵⁴⁶

1179. The IRGC also supported al-Qaeda through its proxy, Hezbollah. As the *Washington Post* reported at the time in 2002, the IRGC's lead terrorist proxy, Hezbollah, was "increasingly teaming up with al Qaeda on logistics and training for terrorist operations, according to U.S. and European intelligence officials and terrorism experts."⁵⁴⁷ "The new cooperation ... includes coordination on explosives and tactics training, money laundering, weapons smuggling and acquiring forged documents, according to knowledgeable sources. This new alliance, even if informal, has greatly concerned U.S. officials in Washington and intelligence operatives abroad who believe the assets and organization of Hezbollah's formidable militant wing will enable a hobbled al Qaeda network to increase its ability to launch attacks against American targets."⁵⁴⁸

1180. The "collaboration" between the IRGC (through Hezbollah) and al-Qaeda "illustrate[d] what analysts [said] [was] an evolving pattern of decentralized alliances between terrorist groups and cells that share[d] enough of the same goals to find common ground: crippling the United States, and forcing the U.S. military out of the Middle East and Israel out of Palestinian territory. 'There's a convergence of objectives,' said Steven Simon, a former National Security Council terrorism expert."⁵⁴⁹ As the *Washington Post* reported, "[a]lthough cooperation between al Qaeda and Hezbollah may have been going on at some level for years, the U.S. war against al

⁵⁴⁵ *Id.*

⁵⁴⁶ *Country Reports on Terrorism 2017* at Foreword.

⁵⁴⁷ Dana Priest and Douglas Farah, *Terror Alliance Has U.S. Worried; Hezbollah, Al Qaeda Seen Joining Forces*, *Washington Post* (June 30, 2002), 2002 WLNR 15332564.

⁵⁴⁸ *Id.*

⁵⁴⁹ *Id.*

Qaeda [] hastened and deepened the relationship. U.S. officials believe that after al Qaeda was driven from Afghanistan, leader Osama bin Laden sanctioned his operatives to ally themselves with helpful Islamic-based groups, said a senior administration official with access to daily intelligence reports.”⁵⁵⁰ The *Post* concluded:

European and U.S. intelligence operatives on the ground in Africa and Asia said they have been trying to convince headquarters of the new alliances but have been rebuffed. “We have been screaming at them for more than a year now, and more since September 11th, that these guys all work together,” an overseas operative said. “What we keep hearing back is that it can’t be because al Qaeda doesn’t work that way. *That is [expletive]*. Here, on the ground, these guys all work together as long as they are Muslims. There is no other division that matters.”⁵⁵¹

1181. Al-Qaeda’s alliance with Hezbollah continued at all times and proved the intelligence operatives on the ground were right. In 2012, the Council on Foreign Relations reported that “al-Qaeda ha[d] stepped up its cooperation on logistics and training with Hezbollah, a radical, Iran-backed Lebanese militia drawn from the minority Shiite strain of Islam.”⁵⁵²

1182. On or about August 7, 2020, on the anniversary of the IRGC/al-Qaeda bomb attack against U.S. embassies in Africa, Israeli commandos acting at the request of the United States killed al-Qaeda’s number 2 leader, Abu Muhammad al-Masri, in a covert mission in Tehran.⁵⁵³ Masri was in Iran as a guest of the Iranian government and was permitted to freely plan attacks against the United States from an IRGC-provided safe haven in Tehran. The timing of the attack was not a coincidence, but a rather a professional slap in the terrorists’ face extended by the U.S. and Israeli governments to the IRGC and al-Qaeda, as the latter allies suffered an embarrassing and catastrophic loss on the anniversary of one of their greatest terrorist triumphs.

⁵⁵⁰ *Id.*

⁵⁵¹ *Id.*

⁵⁵² *al-Qaeda (a.k.a. al-Qaida, al-Qa`ida)*, Council on Foreign Relations (June 6, 2012).

⁵⁵³ Goldman at al., *Al Qaeda’s No. 2, Accused in U.S. Embassy Attacks, Was Killed in Iran*.

1183. The close relationship between al-Qaeda and the IRGC has continued in recent years. In 2017, the U.S. State Department explained, “Since at least 2009, Iran has allowed AQ facilitators to operate a core facilitation pipeline through the country, enabling AQ to move funds and fighters to South Asia and Syria.”⁵⁵⁴ It further accused the IRGC of remaining unwilling to bring to justice or identify al-Qaeda members in its custody.⁵⁵⁵ The next year, the agency reaffirmed those conclusions and reiterated the IRGC’s close relationship with al-Qaeda.⁵⁵⁶

1184. By supporting al-Qaeda and the Taliban, the IRGC provided material support and resources for the attacks that killed or injured Plaintiffs or members of their families. Al-Qaeda and the Taliban directly participated in the attacks that killed or injured Plaintiffs or their family members. Moreover, the IRGC was closely intertwined with al-Qaeda and the Taliban and associated terrorist groups acting in Afghanistan, and the IRGC provided weapons, funding, training, cell phones, and logistical support al-Qaeda and the Taliban. Material support and resources provided to the IRGC thus also flowed to al-Qaeda and the Taliban, causing the injury and deaths of Plaintiffs or their family members.

1185. The mafia-style “syndicate” of which both the Taliban and al-Qaeda formed a part made attacks by each group more lethal. The IRGC’s mutually reinforcing support for both the Taliban and al-Qaeda made both organizations more effective.

1186. By supporting al-Qaeda, the IRGC provided material support and resources for the extrajudicial killings that killed or injured Plaintiffs or members of their families. Al-Qaeda directly participated in many of the attacks that killed or injured Plaintiffs or their family

⁵⁵⁴ U.S. State Dep’t, *Country Reports on Terrorism 2016* at Iran Section (July 2017).

⁵⁵⁵ *Id.*

⁵⁵⁶ *Country Reports on Terrorism 2017* at Foreword.

members. Moreover, al-Qaeda was closely intertwined with the Taliban and associated terrorist groups acting in Afghanistan, and al-Qaeda planned and authorized the Taliban attacks in which it did not directly participate. Material support and resources provided to al-Qaeda thus flowed to the Taliban, causing the injury and deaths of Plaintiffs or their family members.

B. In Furtherance Of The IRGC Conspiracy, Al-Qaeda Authorized And Planned The Attacks That Injured Plaintiffs

1187. Since at least the mid-2000s, al-Qaeda authorized and planned the Taliban's attacks on U.S. forces in Afghanistan in several ways.

1. Al-Qaeda Authorized the Attacks that Injured Plaintiffs

1188. Al-Qaeda provided critical religious authorization for Taliban attacks on U.S. forces. As noted above, in 1998 bin Laden himself directed all Muslims to kill Americans at every opportunity. In the ensuing years, senior al-Qaeda leaders issued a series of *fatwas* directed toward the Taliban, conferring religious permission for them to attack Americans in Afghanistan.

1189. After bin Laden was killed in May 2011, about three months prior to the first attack on a Plaintiff, the Taliban confirmed bin Laden's religious and moral authority over their Afghan jihad, stating: "Osama Bin Laden You were the *sheikh of the Umma*, a zealous man, and *the scholar and imam of the nation at the level of Jihad* and the fighting of the enemies and their minions. You were *our* sheikh, *our* imam and *role model*, the *hero and miracle of our times, unique* among your peers, *pious and highly sensible*."⁵⁵⁷

1190. Consistent with all these activities, al-Qaeda operatives often assumed a position of moral, religious, and tactical authority over Taliban members. Al-Qaeda members, for

⁵⁵⁷ Al-Somood, *Bin Laden Is Alive O Dead Ones And The Cowards Should Not Dare Close Their Eyes* (July 1, 2011) (emphasis added).

example, often “act[ed] as instructors and religious teachers for Taliban personnel and their family members.”⁵⁵⁸

1191. Al-Qaeda also authorized the Taliban’s terrorist attacks through its participation in Syndicate, which involved periodic mafia-style meetings in which al-Qaeda, the Taliban, and other members of the syndicate (such as Lashkar-e-Taiba) would confer about geographies and targets to attack.⁵⁵⁹ The Syndicate jointly authorized particular types of terrorist attacks in particular geographies to be carried out by the syndicate’s individual members. Among other things, the Syndicate specifically approved: (1) the creation and operation of the Kabul Attack Network to attack Americans in Kabul and the surrounding provinces; (2) the campaign of suicide attacks against Americans throughout Afghanistan; (3) the Taliban’s campaign of using anti-American IED and suicide attacks specifically in Nangarhar, Nuristan, Kunar and Laghman (“N2KL”) Provinces and P2K; (4) the Taliban’s “surge” in Kandahar and Helmand from 2010 through 2012; and (5) the Syndicate’s use of, and later aggressive focus on, CAN fertilizer bomb attacks specifically targeting Americans.

1192. Al-Qaeda’s messages of authorization were particularly influential with respect to suicide bombings. In February 2003, bin Laden issued a recording calling specifically for suicide attacks in Afghanistan and Iraq. A few months later, he reiterated in a *fatwa* directed at Afghans that “jihad against [the Coalition] is your duty” and that, “If you start suicide attacks, you will see the fear of Americans all over the world.”⁵⁶⁰ Afghan terrorists had previously viewed suicide

⁵⁵⁸ Thomas Joscelyn, *Al Qaeda Growing Stronger Under Taliban’s Umbrella, UN Finds*, Long War J. (June 23, 2019) (“*Al Qaeda Growing Stronger*”).

⁵⁵⁹ See *The al Qaeda – Taliban Connection*.

⁵⁶⁰ *Osama bin Laden: Calls for Martyrdom Operations Against US and British Interests* (Apr. 10, 2003) (emphasis added).

attacks as taboo, but al-Qaeda convinced it that such attacks were religiously permissible.

Al-Qaeda trumpeted that success online, announcing, “While suicide attacks were not accepted in the Afghani culture in the past, they have now become a regular phenomenon!”⁵⁶¹ With al-Qaeda’s authorization, the number of suicide attacks in Afghanistan increased from one in 2002, two in 2003, and six in 2004 to 21 in 2005, and more than 100 in 2006. Thereafter, suicide bombings remained a cornerstone of the Taliban’s strategy.

1193. As a result, al-Qaeda’s role in that suicide-bombing trend was pivotal and was the but-for cause of each Taliban suicide bomb attack.

1194. Al-Qaeda also authorized the Taliban’s use of IED attacks against Americans in Afghanistan, and bin Laden regularly called for terrorists to attack Americans with IEDs.

2. Al-Qaeda Planned the Attacks that Injured Plaintiffs

1195. Al-Qaeda also planned the Taliban’s terrorist attacks against Americans in Afghanistan. Working through its Syndicate partners and from its safe havens on both sides of the Afghanistan-Pakistan border, al-Qaeda “plan[ned] international as well as regional terrorist attacks, particularly in Afghanistan.”⁵⁶² Two terrorism scholars explained al-Qaeda’s syndicate-related shuras as follows:

The staying power of al-Qaeda became rooted in its ability to draw from and coordinate with allied groups embedded in multiple networks on both sides of the border. . . . It established a number of shuras to ***coordinate strategy, operations, and tactics*** against the West and regional allied governments. In particular, al-Qaeda fighters have been involved in ***planning and carrying out suicide attacks, developing improved explosive devices, and helping conduct operations*** against high-value targets.⁵⁶³

⁵⁶¹ Brian Glyn Williams, *Suicide Bombings in Afghanistan* at 5, Jane’s Islamic Affairs Analyst (Sept. 2007).

⁵⁶² *Resilient al-Qaeda* at 3.

⁵⁶³ *Id.* at 3-4.

1196. Al-Qaeda training provided another key mechanism through which that planning occurred. Before the September 11 attacks, al-Qaeda operated training camps in eastern Afghanistan at the Taliban's request. By 2005 at the latest, al-Qaeda began bringing instructors from Iraq to train the Taliban how to fight Americans. At all relevant times, these al-Qaeda camps trained terrorists in the al-Qaeda signature of turning fertilizer into bombs.

1197. By the mid-2000's, al-Qaeda's partnership with the Haqqani Network had facilitated the emergence of a network of al-Qaeda training camps in North Waziristan, many of which were also affiliated with Sirajuddin Haqqani.⁵⁶⁴

1198. The training continued throughout the relevant timeframe of this case. In 2015, for example, U.S. and Afghan forces raided two al-Qaeda training camps in Kandahar Province – both reportedly “hosted by the Taliban.”⁵⁶⁵ One camp was the largest al-Qaeda facility discovered since the September 11 attacks, occupying nearly 30 square miles. On information and belief, this camp trained terrorists in how to make CAN fertilizer bombs and included an on-site al-Qaeda CAN fertilizer bomb factory.

1199. Working jointly with polyterrorist Sirajuddin Haqqani, al-Qaeda specifically planned the Kabul Attack Network's campaign of terror, including its suicide bomber attacks. As two terrorism scholars explained, the “operational and tactical cooperation” provided by

⁵⁶⁴ Def. Intelligence Agency, *Intelligence Information Report: Location and Activities of the Training Centers Affiliated with the Haqqani Network, Taliban, and al-Qaeda in Northern Waziristan and Future Plans and Activities of Sarajuddin ((Haqqani))* (Apr. 16, 2008) (listing training camps and some of the terrorists there).

⁵⁶⁵ Thomas Joscelyn & Bill Roggio, *Trump's Bad Deal With The Taliban*, Politico (Mar. 18, 2019).

al-Qaeda “increased the ability of the Haqqani Network to carry out sophisticated attacks in Kabul,” “through operations [that al-Qaeda] planned together with Sirajuddin Haqqani.”⁵⁶⁶

1200. Al-Qaeda also planned the Taliban’s attacks by devising the operational scheme for them. Information derived from al-Qaeda and Taliban detainees held at Guantanamo Bay, Cuba (“Gitmo”) corroborates those activities. For example, according to purported Gitmo intelligence files quoted by terrorism experts Bill Roggio and Thomas Joscelyn, one detainee, Abdul Razak, was “a high-level military commander in a newly-conceived ‘unification’ of Al Qaeda, [Hezb-e-Islami Gulbuddin (“HIG”)] and Taliban forces within Afghanistan,” which the groups’ respective leaders conceived during a meeting in Pakistan in early spring 2003.⁵⁶⁷ Another Gitmo detainee files similarly documented “joint operations meeting[s]” where the participants, which included al Qaeda, Taliban and LT commanders “decided to increase terrorist operations in the Kapisa, Kunar, Laghman, and Nangarhar provinces, including suicide bombings, mines, and assassinations.”⁵⁶⁸ Together, these reports “demonstrate a high degree of collusion between al Qaeda and other terrorist groups” as part of a “jihadist hydra” that shared the “common goal” of seeking to “drive the U.S.-led coalition out of Afghanistan.”⁵⁶⁹

1201. Al-Qaeda also taught the Taliban effective terrorist tradecraft. Through its relationship with al-Qaeda, the Taliban “developed or acquired new commercial communications gear and field equipment,” as well as “good tactical, camouflage, and marksmanship training.”⁵⁷⁰ They also “share[d] communication and transportation routes, coordinate[d] attacks, and even

⁵⁶⁶ *Resilient al-Qaeda* at 9.

⁵⁶⁷ *The al Qaeda – Taliban Connection*.

⁵⁶⁸ *Id.* (brackets in original).

⁵⁶⁹ *Id.*

⁵⁷⁰ *Id.* at 293.

utilize[d] the same explosive and suicide-bomber networks.”⁵⁷¹ The Taliban’s (including its Haqqani Network’s) effective terrorist tradecraft was essential to its ability to execute al-Qaeda’s nationwide CAN fertilizer bomb campaign, which depended upon sophisticated logistics, communications, smuggling, storage, and other technical skills that the Taliban only acquired through its relationship with al-Qaeda.

1202. All these activities were part of al-Qaeda’s planning of the Taliban’s CAN fertilizer bomb attacks in Afghanistan. By providing an array of advice, direction, and material support to the Taliban, al-Qaeda was able to use the Taliban for its own jihadist ends. In so doing, al-Qaeda followed its more general practice of planning terrorist attacks whose details it would delegate to local Islamic proxies. As terrorism scholar Thomas Ruttig observed: “Both in Afghanistan and Pakistan, al-Qaeda exploits local conditions by co-opting militant groups with local battle experience.”⁵⁷² Here, its “cooptation” of the Taliban was especially effective.

1203. Al-Qaeda’s planning activities extended specifically to the two CAN fertilizer bomb attack types that account for every attack in this case: IEDs and suicide bombs.

i. Al-Qaeda Planned the IED Attacks that Injured Plaintiffs

1204. Al-Qaeda planned the Taliban’s campaign of IED attacks in Afghanistan in which the explosive was ammonium nitrate derived from CAN Fertilizer manufactured, sold, and distributed by Fatima and/or Pakarab. In this Complaint, Plaintiffs describe the CAN fertilizer made by Fatima and by Pakarab, collectively, as “Fatima CAN Fertilizer” or “Fertilizer.”

1205. At all relevant times, al-Qaeda was the world leader amongst Sunni terrorist groups with respect to converting fertilizer into ammonium nitrate for use in CAN fertilizer

⁵⁷¹ *Resilient al-Qaeda* at 9.

⁵⁷² Thomas Ruttig, *The Other Side* at 22, Afghanistan Analysts Network (July 2009) (“*Ruttig, The Other Side*”).

bomb attacks against Western targets. As Senator Charles Schumer stated in 2004, “bombs using [CAN] [were] the weapon of choice of al-Qaida.”

1206. From 2001 through 2016, al-Qaeda supported fertilizer-based bomb strategies in every theater in which al-Qaeda pursues terrorist attacks against America and its allies. As one journalist wrote in 2007, “[i]n the new age of Islamist terrorism, [CAN] fertiliser packed into a truck with plastic explosive as a detonator has also become an al Qaida trademark.”⁵⁷³

1207. CAN fertilizer bombs were also a literal part of al-Qaeda’s terrorism playbook, and al-Qaeda regularly instructed Taliban, including Haqqani Network, terrorists, in person and in writing, regarding CAN fertilizer bombs. For example, a 39-page al-Qaeda memo recovered from an al-Qaeda laptop in Pakistan in 2004 provided that military explosives were often impractical to acquire, and instructed instead that jihadists should use home-made explosives, including ammonium nitrate bombs derived from CAN fertilizer.

1208. Al-Qaeda and the Haqqani Network agents, operatives, and fronts in Afghanistan and Pakistan facilitated al-Qaeda’s CAN fertilizer bomb infrastructure by purchasing every essential element of the Syndicate’s bombmaking enterprise and managing the transportation and logistics of vast volumes of bombs and bomb precursors. These Syndicate front companies serviced the litany of joint al-Qaeda / Haqqani Network bombmaking factories and training camps in eastern Afghanistan and Syndicate-controlled territory in Afghanistan and Pakistan. It did so because the Haqqani Network have historically played a key role in obtaining and securing bomb components and precursors for use by al-Qaeda bombmakers operating in camps

⁵⁷³ David Barrett, *Deadly Fertiliser Bombs Used By Terrorists Worldwide*, Press Association News (Apr. 30, 2007).

in Afghanistan and Pakistan jointly run by al-Qaeda and the Haqqani Network under the leadership of Syndicate polyterrorists like Sirajuddin Haqqani.

1209. While al-Qaeda and Haqqani Network fronts and agents were sourcing their key explosive ingredient exclusively from Fatima and Pakarab, al-Qaeda forward-deployed terrorist trainers in Afghanistan and Pakistan specifically instructed the Taliban to acquire Fatima CAN Fertilizer, convert it into an ammonium nitrate bomb, and use the resulting weapon to kill and maim Americans in Afghanistan.

1210. Al-Qaeda's plan for the nationwide deployment of CAN fertilizer bombs against Americans in Afghanistan also included aggressive support by al-Qaeda bombmakers and logisticians in Pakistan, aided by their Taliban, including Haqqani Network, allies, to maintain a series of joint al-Qaeda/Taliban (including through the Haqqani Network) bombmaking sites, where the purpose was specifically to construct large volumes of CAN fertilizer bombs detonated via a Syndicate IED or suicide bomber. In so doing, bin Laden and his Taliban allies, including its Haqqanis, were reprising one of their celebrated roles against the Soviets during the Afghan war, when they worked together to help ar the mujaheddin with key anti-armor weapons.

1211. By 2009, according to famed journalist Peter Bergen, al-Qaeda's strategy to teach the Taliban how to turn CAN fertilizer into CAN fertilizer bombs to kill Americans in Afghanistan was widely known:

[I]n recent years, Taliban leaders have drawn especially close to Al Qaeda. . . . Today, at the leadership level, the Taliban and Al Qaeda function *more or less as a single entity*. The signs of this are everywhere. For instance, IED attacks in Afghanistan have increased dramatically since 2004. What happened? As a Taliban member told Sami Yousafzai and Ron Moreau of *Newsweek*, "*The Arabs taught us how to make an IED by mixing nitrate fertilizer and diesel fuel and how to pack plastic explosives and to connect them to detonators and remote-*

control devices like mobile phones. We learned how to do this blindfolded so we could safely plant IEDs in the dark.”⁵⁷⁴

1212. At all relevant times, dual al-Qaeda/Haqqani Network operative Sirajuddin Haqqani planned the Syndicate’s CAN fertilizer bombing campaign, and focused above all else on producing a regular, reliable, and deadly supply of CAN fertilizer bombs for use in Syndicate IED and suicide bomb attacks targeting Americans in Afghanistan.

1213. Like his al-Qaeda brothers, Sirajuddin Haqqani viewed the Syndicate’s CAN fertilizer bomb campaign infrastructure as a key source of al-Qaeda and Haqqani Network power in Afghanistan and Pakistan, and leverage over other members of the Syndicate. Consequently, al-Qaeda and Haqqani Network operatives, including Sirajuddin Haqqani and other Haqqani family members, closely oversaw the core commercial and financial relationships that enabled Syndicate’s regular and reliable flow of Fatima CAN Fertilizer for conversion into CAN fertilizer bombs. This close involvement by senior al-Qaeda and Haqqani Network leadership ensured a tight nexus between Defendants’ reckless financial services to al-Qaeda and Haqqani Network agents, operatives, and fronts and the Syndicate’s CAN fertilizer bomb infrastructure.

1214. In this relationship, the Haqqani Network provided the location, support, and funding for the CAN fertilizer bombmaking sites, while al-Qaeda bombmakers presided over an assembly line of explosives creation in which bombmakers would convert Fatima CAN Fertilizer into CAN fertilizer bombs.

1215. Once al-Qaeda’s bombmakers had cooked down Fatima CAN Fertilizer into ammonium nitrate, al-Qaeda would then prepare the ammonium nitrate to be used in one or more CAN fertilizer bombs derived from al-Qaeda schematics, including: (1) large CAN fertilizer-

⁵⁷⁴ *The Front* (emphases added).

based IEDs specifically designed to destroy an American armored vehicle; (2) small CAN fertilizer-based IEDs specifically designed to kill or maim Americans on foot; and (3) CAN fertilizer-based suicide vests and suicide VBIEDs specifically designed to take out the largest possible American armor, or to be deployed as part of a complex attack targeting an American installation. Different bomb types require different component parts, and therefore al-Qaeda's bombmakers would coordinate the correct parts with the correct designs to ensure maximal effect. Once al-Qaeda's designed- and manufactured-CAN fertilizer bombs were completed, al-Qaeda and the Haqqani Network would distribute the CAN fertilizer bombs to the relevant Syndicate terrorist cells throughout Afghanistan to blow up Americans.

1216. More broadly, al-Qaeda members regularly trained the Taliban's, including its Haqqani Network's, commanders in sophisticated CAN fertilizer bomb-making techniques that were material to the terrorists' ability to assemble and deploy explosives against Coalition forces. According to the terrorist scholar Seth Jones:

Insurgent groups also used al Qaeda support to construct increasingly sophisticated [IEDs], including remote controlled detonators. For example, al Qaeda ran a handful of manufacturing sites in the Bush Mountains, the Khamran Mountains, and the Shakai Valley in Pakistan's Federally Administered Tribal Areas. They ranged from small facilities hidden within compounds that build IEDs to much larger "IED factories" that doubled as training centers and labs whose recruits experimented with IED technology. Some of this explosives expertise came from Iraqi groups that provided information on making and using various kinds of remotely controlled devices and timers.⁵⁷⁵

1217. Al-Qaeda's support of the Taliban's, including its Haqqani Network's IED attacks also included the use of forward deployed al-Qaeda terrorist trainers throughout Afghanistan. For example, by 2010, "[i]n southern Afghanistan, there [were] pockets of al Qaeda . . . in Helmand and several neighboring provinces, such as Kandahar and Zabol," which helped the Taliban

⁵⁷⁵ *Graveyard Of Empires* at 292.

“conduct suicide attacks and other [IED]” attacks.⁵⁷⁶ Al-Qaeda also forward deployed IED terrorist trainers in P2K and N2KL. At all times, al-Qaeda’s forward deployed trainers directed its CAN fertilizer bomb campaign in keeping with CAN fertilizer bombing’s status as a “signature” al-Qaeda attack type.

1218. Al-Qaeda’s planning efforts were significant and amplified the lethality of the Taliban’s, including its Haqqani Network’s, attacks. Indeed, al-Qaeda’s ability to export its terrorism expertise to local groups is what “renders al-Qaeda effective in the first place.”⁵⁷⁷ In the case of the Taliban and the Haqqani Network, al-Qaeda executed the “transfer of technical knowhow, devices, and training for IED use, truck and suicide bombings as well as the channel[ing] of what some observer[s] call ‘strategic-level funding.’”⁵⁷⁸ Those activities were material to the Taliban’s and Haqqani Network’s ability to execute the type of attacks that killed and injured Plaintiffs. As Mr. Ruttig concluded, al-Qaeda’s activities “raise[d] the level of sophistication of Taleban and associated networks’ operations.”⁵⁷⁹

1219. As Mr. Bergen put it in November 2009, “Small numbers of Al Qaeda instructors embedded with much larger Taliban units have functioned something like U.S. Special Forces do – as trainers and force multipliers.”⁵⁸⁰ Al-Qaeda’s sophistication and support was important to the Taliban’s (including its Haqqani Network’s) terrorist enterprise. And al-Qaeda’s involvement went beyond technical support; it also worked actively with Taliban leadership to set strategy

⁵⁷⁶ *Id.* at 330.

⁵⁷⁷ Thomas Ruttig, *The Other Side* at 22, Afghanistan Analysts Network (July 2009) (“*Ruttig, The Other Side*”).

⁵⁷⁸ *Id.*

⁵⁷⁹ *Id.*

⁵⁸⁰ *The Front*.

and orchestrate attacks. For that reason, “Al Qaeda leader Ayman al-Zawahiri, Hamza bin Laden and the Taliban leadership ‘have repeatedly emphasized the importance of the alliance between’ the two groups.”⁵⁸¹

ii. Al-Qaeda Planned the Suicide Attacks that Injured Plaintiffs

1220. Al-Qaeda’s planning activities extended to suicide bombings. The suicide attacker is a core component of al-Qaeda’s ideology and operational philosophy. Al-Qaeda exported its suicide-bombing expertise to the Taliban through their joint syndicate, and in so doing played a pivotal leadership and operational role in every Taliban suicide bombing in Afghanistan during the relevant time. For that reason, every suicide bombing alleged in this case was jointly planned and committed by al-Qaeda and the Taliban.

1221. Al-Qaeda planned suicide bombings in Afghanistan by mounting a coordinated communications campaign to persuade Taliban (including Haqqani) terrorists to embrace suicide attacks against Americans. This campaign included messages touting suicide attacks and honoring “martyrs” through al-Qaeda print and video outlines; promoting religious “scholarly” outreach; and emphasizing in-person indoctrination of Taliban and Haqqani leadership.

1222. Al-Qaeda used this message – and the moral authority conveyed by bin Laden’s 2003 *fatwa* authorizing martyrdom operations – to change the Taliban’s (including its Haqqani Network’s) organizational posture toward suicide bombing. As Dr. Jones summarized the evidence, “Al Qa’ida’s involvement was particularly important in this regard.”⁵⁸²

1223. To implement its planned suicide-bombing campaign, al-Qaeda also created and ran training camps that converted disaffected recruits into suicide bombers at an industrial scale.

⁵⁸¹ *Al Qaeda Growing Stronger*.

⁵⁸² *Graveyard of Empires* at 293.

In collaboration with other syndicate members, Al-Qaeda created and designed a process for identifying candidates for martyrdom operations; indoctrinating them with the necessary religious and socio-political concepts; and training them how, for example, to conceal the explosives in a Suicide VBIED, navigate a checkpoint, and detonate for maximum impact. Some of this training occurred in al-Qaeda-affiliated camps in Pakistan.

1224. To carry-out their joint suicide bombing campaign, al-Qaeda and the Taliban relied upon a series of dual-hatted al-Qaeda/Taliban terrorists to support the key nodes of the training and recruitment effort, including the madrassas from which most recruits were drawn and the training camps in which they were refined into suicide weapons. Such dual-hatted al-Qaeda/Taliban terrorists include, but are not limited to:

- **Sirajuddin Haqqani**, a member of al-Qaeda’s military council and commander of the Haqqani Network, who has stated that al-Qaeda “enlighten[s] the road for [the Taliban] and they resist against the cross worshippers [*i.e.*, the Americans] by cooperating with us and us with them in one trench,” pursuant to cooperation “at the highest limits”⁵⁸³;
- **Qari Ziaur Rahman**, a dual-hatted al-Qaeda/Taliban terrorist who was a top regional commander of both organizations in Kunar and Nuristan Provinces; and
- **Sheikh Aminullah (aka Fazeel-a-Tul Shaykh Abu Mohammed Ameen al Peshwari)**, a dual-hatted al-Qaeda/Taliban terrorist who ran the Ganj Madrassa, which trained and recruited suicide bombers for al-Qaeda and the Taliban.

1225. Al-Qaeda also created the suicide network infrastructure necessary to deploy al-Qaeda suicide bombers, and the suicide bombs they detonated, in support of the Taliban’s jihad against Americans in Afghanistan. The Syndicate’s suicide attack infrastructure included: (1) high-level meetings between representatives of al-Qaeda, the Taliban, and other members of the Syndicate; (2) joint al-Qaeda/Taliban safe houses and ratlines to support the deployment of suicide bombers inside Afghanistan; (3) joint al-Qaeda/Taliban explosives factories, in which the

⁵⁸³ *Taliban Cooperation*.

Syndicate converted Fatima CAN Fertilizer into ammonium nitrate for use in suicide vests and suicide VBIEDs; (4) joint al-Qaeda/Taliban suicide VBIED development sites, in which al-Qaeda and Taliban bombmakers married the CAN fertilizer bomb with a vehicle to create a suicide VBIED; and (5) a constellation of al-Qaeda-affiliated propaganda outlets that glorified the attackers, which was essential both for increasing the likelihood that a particular attacker would carry out his or her attack, as well as incentivizing the next generation of suicide bombers.

1226. As a reflection of the joint nature of al-Qaeda-Taliban martyrdom operations, al-Qaeda suicide bombers were often referred to as “Mullah Omar’s Missiles.” By following a strategy in which the weapons (*i.e.*, the suicide bomber) was created by al-Qaeda and then deployed by the Taliban, both organizations played to their respective operational competencies to maximize the impact of their shared jihad against Americans in Afghanistan. Indeed, when a suicide bomber detonated a CAN fertilizer bomb, as happened in every suicide bomb attack in this case, al-Qaeda created both the suicide bomber and the explosive device itself.

C. In Furtherance Of The IRGC Conspiracy, Al-Qaeda Committed Terrorist Attacks That Killed And Injured Plaintiffs In Joint Cells With The Taliban, Lashkar-E-Taiba, and Jaish-E-Mohammed

1227. Working together, the Syndicate terrorist groups committed every IED and suicide bomb attack in this case. Consistent with bin Laden’s playbook, al-Qaeda provided the technical expertise, training, ratlines, forward deployed support in Afghanistan, and fundraising support, while the Taliban (including its Haqqani Network), Lashkar-e-Taiba, and Jaish-e-Mohammed provided training camps, safe houses, front companies to purchase components, and the terrorists to be trained by al-Qaeda to attack Americans in Afghanistan.

1228. Al-Qaeda members also committed attacks alongside the Taliban, including some of the attacks that killed or injured Plaintiffs or their family members. In fact, many terrorist operatives were “dual-hatted,” meaning that they were both al-Qaeda and Taliban members.

Those dual-hatted terrorists directly committed many of the attacks that killed and injured Plaintiffs. Examples are set forth below.

1. The “N2KL” Provinces: Al-Qaeda Committed the Attacks in Nangarhar, Nuristan, Kunar and Laghman that Injured Plaintiffs

1229. Al-Qaeda deployed senior operatives to coordinate attacks in the strategically critical (and contiguous) Nangarhar, Nuristan, Kunar and Laghman Provinces (known as the “N2KL Provinces” or “N2KL”), which were well-known al-Qaeda strongholds. In N2KL, al-Qaeda, the Taliban, and Lashkar-e-Taiba maintained joint cells responsible for anti-American terrorism, each of which executed the Syndicate’s CAN fertilizer bomb campaign in Afghanistan. The dual-hatted al-Qaeda/Taliban polyterrorists who ran these joint cells included:

- (i) **Farouq al-Qahtani**, al-Qaeda’s “emir for eastern Afghanistan” who “supported the Taliban-led insurgency against the Afghan government, US forces and their allies.”⁵⁸⁴
- (ii) **Sakhr al-Taifi**, al-Qaeda’s number two in Afghanistan, who embedded with the Taliban, “coordinate[d] and direct[ed] insurgent attacks against” “coalition troops throughout eastern Afghanistan,” and “supplie[d] weapons and equipment to insurgents.”⁵⁸⁵
- (iii) **Mufti Assad**, an al-Qaeda network and “insurgent leader who controlled al-Qaida terrorists operating in Kunar,” “led dozens of all-Qaida affiliated fighters throughout eastern Afghanistan and coordinated their attacks across the region,” and “was also an explosives expert who” “train[ed] [] insurgents on how to construct and use [IEDs].”⁵⁸⁶
- (iv) **Abdallah Umar al-Qurayshi**, a senior al-Qaeda operative who commanded the joint al-Qaeda/Taliban cells operating in Kunar and Nuristan Provinces.
- (v) **Abu Atta al-Kuwaiti**, a senior al-Qaeda explosives expert who coordinated the Nuristan and Kunar Province al-Qaeda/Taliban joint cells’ IED and suicide bomb attacks.
- (vi) **Abu Ikhlas al-Masri**, an al-Qaeda commander who helped coordinate al-Qaeda / Taliban attacks in Kunar Province from 2008 until his capture in December 2010.

⁵⁸⁴ Thomas Joscelyn, *Pentagon Confirms Death of Senior al Qaeda Leader In Afghanistan*, Long War Journal (Nov. 4, 2016), <https://tinyurl.com/2p859bcj>.

⁵⁸⁵ ISAF Joint Command, *Morning Operational Update*, Def. Visual Info. Distribution Serv. (May 28, 2012).

⁵⁸⁶ ISAF Joint Command, *Morning Operational Update*, Def. Visual Info. Distribution Serv. (Aug. 5, 2012).

- (vii) **Sa'ad bin Abi Waqas**, a senior al-Qaeda leader who “coordinated attacks against coalition forces,” throughout Kunar Province, “conducted training” and helped terrorists with “weapons procurement.”⁵⁸⁷
- (viii) **Abu Hafs al-Najdi (aka Abdul Ghani)**, a senior al-Qaeda operative who directed al-Qaeda operations in Kunar Province, and was responsible for “planning attacks against” “coalition forces” and “directing suicide-bomb attacks targeting U.S. government officials” that were facilitated by his “network” of Taliban terrorists.⁵⁸⁸
- (ix) **Fatah Gul**, an al-Qaeda facilitator who “ran terrorist training camps where insurgents learned how to conduct [IED] attacks” in N2KL Provinces.⁵⁸⁹

2. The “P2K” Provinces: Al-Qaeda Committed the Attacks in Paktia, Paktika, and Khost that Injured Plaintiffs

1230. Like its N2KL Provinces, Paktia, Paktika, Afghanistan’s Khost Provinces (known as the “P2K Provinces” or “P2K”) were a strategically critical area that historically served as a Haqqani Network stronghold and also operated as a “traditional al-Qaeda safe haven[.]”⁵⁹⁰

1231. Al-Qaeda and the Taliban, through the Haqqani Network, maintained joint cells responsible for anti-American terrorism in P2K, each of which executed the Syndicate’s CAN fertilizer bomb and suicide campaign in Afghanistan. The dual-hatted al-Qaeda/Taliban polyterrorists who ran these P2K-related joint cells included:

- (i) **Sirajuddin Haqqani**, a member of al-Qaeda’s military council, leader of the Quetta Shura Taliban, and commander of the Haqqani Network;
- (ii) **Bekkay Harrach (aka al-Hafidh Abu Talha al-Almani)**, a senior member of al-Qaeda’s external operations branch, who specifically planned, authorized, and helped commit Haqqani Network attacks while living under the direct protection of Siraj Haqqani, himself a member of al-Qaeda’s military council; and
- (iii) **Khalil al-Rahman Haqqani**, Jalaluddin Haqqani’s brother and a dual-hatted al-Qaeda/Taliban terrorist, serving as a “fundraiser, financier, and operational

⁵⁸⁷ ISAF Joint Command, *Morning Operational Update*, Def. Visual Info. Distribution Serv. (Apr. 16, 2011).

⁵⁸⁸ U.S. Dep’t of Def., *Strike Kills No. 2 Insurgent in Afghanistan* (Apr. 26, 2011).

⁵⁸⁹ ISAF Joint Command, *Morning Operational Update* (Aug. 5, 2012).

⁵⁹⁰ *Resilient al-Qaeda* at 11-12.

commander” for the Haqqani Network,⁵⁹¹ as well as an agent who “acted on behalf of al-Qa’ida”⁵⁹² and had “been linked to al-Qa’ida terrorist operations.”⁵⁹³

3. **Kabul Attack Network-Related Provinces: Al-Qaeda Committed the Kabul Attack Network Attacks that Injured Plaintiffs**

409. Al-Qaeda deployed senior operatives to coordinate attacks in the strategically critical cluster of provinces around the capital city. This area was the focus of the Kabul Attack Network, where al-Qaeda and the Taliban, maintained joint al-Qaeda/Taliban cells that planned and committed terrorist attacks, each of which executed the Syndicate’s CAN fertilizer bomb and/or suicide attack campaign in Kabul Attack Network-related provinces. Such dual-hatted al-Qaeda/Taliban polyterrorists who ran the cells included:

- (i) **Sirajuddin Haqqani**, a member of al-Qaeda’s military council, senior leader of the Quetta Shura Taliban, and commander of the Haqqani Network; and
- (ii) **Ahmed Jan Wazir**, a dual-hatted al-Qaeda/Taliban terrorist who, in 2008, was named commander of jihadist forces in Ghazni Province by both al-Qaeda and the Taliban.

⁵⁹¹ Bill Roggio, *US Designates al Qaeda, Haqqani Network Leaders As Terrorists*, Long War J. (Feb. 9, 2011).

⁵⁹² Press Release, U.S. Dep’t of Treasury, *Treasury Targets The Financial And Support Networks of Al Qa’ida And The Taliban, Haqqani Network Leadership* (Feb. 9, 2011).

⁵⁹³ Press Release, U.S. Dep’t of State, *Rewards for Justice - Reward Offers for Information on Haqqani Network Leaders* (Aug. 20, 2014).

X. THE IRGC-BACKED TALIBAN TERRORIST SYNDICATE IN AFGHANISTAN AND PAKISTAN LED BY AL-QAEDA AND THE TALIBAN KILLED AND INJURED THE PLAINTIFFS WHO WERE ATTACKED IN AFGHANISTAN IN 2012 THROUGH 2018 THROUGH TERRORIST ATTACKS FOR WHICH DEFENDANTS PROVIDED SUBSTANTIAL ASSISTANCE

410. Plaintiffs are American civilians, servicemembers, and contractors serving in Afghanistan, and their family members, who were killed or injured in terrorist attacks committed by al-Qaeda (a designated FTO at the time), the Taliban, including its Haqqani Network (a designated FTO at the time), Lashkar-e-Taiba (a designated FTO at the time), and Jaysh-e-Mohammed (a designated FTO at the time), all of which collaborated in a terrorist alliance, known as the “Syndicate,” that was funded, armed, and logistically supported by Hezbollah, the Qods Force, and Regular IRGC.

411. Hezbollah, the Qods Force, and Regular IRGC provided key aid to the Syndicate from inception through their victory in 2021. Hezbollah, the Qods Force, and Regular IRGC specifically provided al-Qaeda and the Taliban (including its Haqqani Network) weapons, funds, training, logistical support, communications technology, safe haven, and assistance with narcotics trafficking, which raised money for their shared terrorist enterprise against America (i.e., the conspiracy), which al-Qaeda and the Taliban, including its Haqqani Network, used to aid the terrorists’ ability to execute the attacks that injured Plaintiffs.

412. The embargoed dual-use American technology – including thousands of secure American smartphones every year – hundreds of millions of U.S. Dollars annually, and vast network of logistical and operational support for the Irancell and TCI fronts that MTN Group, MTN Dubai, ZTE Corporation, and Huawei Corporation provided to their counterparties controlled by Hezbollah, the Qods Force, and Regular IRGC flowed through to al-Qaeda, the Taliban (including its Haqqani Network), and their Syndicate allies that committed each attack

that injured each Plaintiff through transfers made by Hezbollah, the Qods Force, and Regular IRGC to al-Qaeda and the Taliban (including its Haqqani Network).

A. April 4, 2012 Attack In Faryab (Families of David W. Lau, Christopher J. Rosebrock, and Nicholas Rozanski)

413. On April 4, 2012, a joint cell of al-Qaeda/Taliban terrorists committed a suicide bomb attack targeting Americans in Faryab⁵⁹⁴ (“April 4, 2012 Suicide Attack”).⁵⁹⁵

414. The April 4, 2012 Suicide Attack was committed by al-Qaeda (an FTO) and the Taliban acting together in a joint al-Qaeda-Taliban cell with al-Qaeda providing, indoctrinating, and training the bomber, who was deployed by the Taliban. On information and belief, the suicide bomber who detonated the bomb during the attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda’s tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return. raining the suicide bomber.

415. On information and belief, the device that the suicide bomber detonated during the April 4, 2012 Suicide Attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor

⁵⁹⁴ In this section, Plaintiffs identify the attack geography by Afghan province. For example, “Faryab” means “Faryab Province, Afghanistan.” If a location represents both a province and a city (e.g., Kabul), Plaintiffs refer to the Provincial-level designation in this section unless otherwise indicated.

⁵⁹⁵ In this section, any reference to “attack” within a specific Plaintiff’s allegations refer to the previously referenced attack concerning such Plaintiff, and are not a reference to any other attack.

ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell’s April 4, 2012 Suicide Attack.

416. The April 4, 2012 Suicide Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1. The David Lau Family

417. Plaintiff Sergeant First Class David Lau served in Afghanistan as a member of the U.S. Army National Guard. SFC Lau was injured during the April 4, 2012 Suicide Attack, which severely wounded SFC Lau, who suffered severe injuries to both his legs requiring three years in a limb salvage program, extensive injuries to his dominant hand including the loss of a finger resulting in diminished function, severe injuries to shoulders and bicep, limb atrophy, dental injuries, loss of hearing, burns, and embedded toxic ball bearings. As a result of the Attack and his injuries, SFC Lau has experienced severe physical and emotional pain and suffering.

418. SFC Lau was a U.S. national at the time of the attack and remains one to this day.

419. Plaintiff Hamide Lau is the wife of SFC Lau and a U.S. national.

420. Plaintiff K.L., by and through his next friend David Lau, is the minor son of SFC Lau and a U.S. national.

421. Plaintiff M.L., by and through her next friend David Lau, is the minor daughter of SFC Lau and a U.S. national.

422. Plaintiff Alexander Lau is the son of SFC Lau and a U.S. national.

423. Plaintiff Vivian Perry is the mother of SFC Lau and a U.S. national.

424. Plaintiff Holly Abraham is the sister of SFC Lau and a U.S. national.

425. Plaintiff Leroy Lau Jr. is the brother of SFC Lau and a U.S. national.

426. Plaintiff Michelle Lee Rauschenberger is the sister of SFC Lau and a U.S. national.

427. Plaintiff Jammie Smith is the sister of SFC Lau and a U.S. national.

428. As a result of the April 4, 2012 Suicide Attack and SFC Lau's injuries, each member of the Lau Family has experienced severe mental anguish, emotional pain and suffering.

2. The Nicholas Rozanski Family

429. Captain Nicholas Rozanski served in Afghanistan as a member of the U.S. Army National Guard. CPT Rozanski was injured during the April 4, 2012 Suicide Attack. CPT Rozanski died on April 4, 2012 as a result of injuries sustained during this attack.

430. CPT Rozanski was a U.S. national at the time of the attack and his death.

431. Plaintiff Alex Rozanski is the brother of CPT Rozanski and a U.S. national.

432. As a result of the attack and CPT Rozanski's injuries and death, each member of the Rozanski Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CPT Rozanski's society, companionship, and counsel.

433. As a result of the attack, CPT Rozanski was injured in his person and/or property. The Plaintiff members of the Rozanski Family are the survivors and/or heirs of CPT Rozanski and are entitled to recover for the damages CPT Rozanski sustained.

3. Christopher Rosebrock

434. Plaintiff Captain Christopher Rosebrock served in Afghanistan as a member of the U.S. Army National Guard. CPT Rosebrock SFC Lau was injured during the April 4, 2012 Suicide Attack, which severely wounded CPT Rosebrock, who suffers from disfiguring shrapnel wounds, muscular atrophy and reduced mobility in his left arm, a concussion, a traumatic brain injury, and blown eardrums. As a result of the attack and his injuries, CPT Rosebrock has experienced severe physical and emotional pain and suffering.

435. CPT Rosebrock was a U.S. national at the time of the attack and remains so today.

B. April 22, 2012 Attack In Ghazni (Michael Metcalf Family)

436. Private First Class Michael Metcalf served in Afghanistan as a member of the U.S. Army. On April 22, 2012, PFC Metcalf was injured in an IED attack in Ghazni. PFC Metcalf died on April 22, 2012 as a result of injuries sustained during the attack.

437. The attack was committed by the Taliban (including its Haqqani Network) and al-Qaeda (an FTO), acting together as a joint cell led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

438. On information and belief, the bomb that the joint cell detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

439. PFC Metcalf's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

440. PFC Metcalf was a U.S. national at the time of the attack and his death.

441. Plaintiff Clarence Metcalf is the father of PFC Metcalf and a U.S. national.

442. Plaintiff Kimberly Metcalf is the mother of PFC Metcalf and a U.S. national.

443. As a result of the April 22, 2012, attack and PFC Metcalf's injuries and death, each member of the Metcalf Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC Metcalf's society, companionship, and counsel.

444. As a result of the April 22, 2012, attack, PFC Metcalf was injured in his person and/or property. The Plaintiff members of the Metcalf Family are the survivors and/or heirs of PFC Metcalf and are entitled to recover for the damages PFC Metcalf sustained.

C. May 6, 2012 Attack In Paktia (Families of Thomas Fogarty and Jonathan Cleary)

445. On May 6, 2012, the Haqqani Network (a part of the Taliban), al-Qaeda (a designated FTO at the time of the attack), and Lashkar-e-Taiba acting together in a joint al-Qaeda-Taliban-Lashkar-e-Taiba cell committed an IED attack targeting Americans in Paktia (“May 6, 2012 IED Attack”).

446. On information and belief, the bomb that the joint cell detonated during the May 6, 2012 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell’s attack.

447. The May 6, 2012 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Thomas Fogarty Family

448. Staff Sergeant Thomas Fogarty served in Afghanistan as a member of the U.S. Army. SSG Fogarty was injured in the May 6, 2012 IED Attack. SSG Fogarty died on May 6, 2012 as a result of injuries sustained during the Attack.

449. SSG Fogarty was a U.S. national at the time of the attack and his death.

450. Plaintiff Stephanie Fisher is the mother of SSG Fogarty and a U.S. national.

451. Plaintiff Thomas Fogarty is the father of SSG Fogarty and a U.S. national.

452. Plaintiff C.F., by and through his next friend Stephanie Fisher, is the minor son of SSG Fogarty and a U.S. national.

453. Plaintiff K.F., by and through his next friend Stephanie Fisher, is the minor son of SSG Fogarty and a U.S. national.

454. As a result of the May 6, 2012 IED Attack and SSG Fogarty's injuries and death, each member of the Fogarty Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Fogarty's society, companionship, and counsel.

455. As a result of the May 6, 2012 IED Attack, SSG Fogarty was injured in his person and/or property. The Plaintiff members of the Fogarty Family are the survivors and/or heirs of SSG Fogarty and are entitled to recover for the damages SSG Fogarty sustained.

2. The Jonathan Cleary Family

456. Plaintiff Corporal Jonathan Cleary served in Afghanistan as a member of the U.S. Army. CPL Cleary was injured in the May 6, 2012 IED Attack, which severely wounded CPL Cleary, who suffers from an amputation of his right leg below the knee. As a result of the May 6, 2012 IED Attack and his injuries, CPL Cleary has experienced severe physical and emotional pain and suffering.

457. CPL Cleary was a U.S. national at the time of the attack and remains so today.

458. Plaintiff April Cleary is the mother of CPL Cleary and a U.S. national.

459. As a result of the May 6, 2012 IED Attack and CPL Cleary's injuries, each member of the Cleary Family has experienced severe mental anguish, emotional pain and suffering.

D. May 7, 2012 Attack In Ghazni (Families of Chase Marta and Jacob Schwallie)

460. On May 7, 2012, a joint cell of al-Qaeda/Taliban/Lashkar-e-Taiba terrorists committed an IED attack against Americans in Ghazni (“May 7, 2012, IED Attack”).

461. The May 7, 2012, IED Attack was committed by the Taliban (including its Haqqani Network) and al-Qaeda (an FTO), acting together as a joint cell led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

462. On information and belief, the bomb that the joint cell detonated during the May 7, 2012, IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell’s attack.

463. The May 7, 2012, IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Chase Marta Family

464. Specialist Chase Marta served in Afghanistan as a member of the U.S. Army. SPC Marta was injured in the May 7, 2012, IED Attack. SPC Marta died on May 7, 2012 as a result of injuries sustained during the May 7, 2012 IED Attack.

465. SPC Marta was a U.S. national at the time of the attack and his death.

466. Plaintiff Karyn Stone is the mother of SPC Marta and a U.S. national.

467. Plaintiff Lawrence Marta is the father of SPC Marta and a U.S. national.

468. Plaintiff Taylor Marta is the sister of SPC Marta and a U.S. national.

469. As a result of the May 7, 2012 IED Attack and SPC Marta's injuries and death, each member of the Marta Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Marta's society, companionship, and counsel.

470. As a result of the May 7, 2012 IED Attack, SPC Marta was injured in his person and/or property. The Plaintiff members of the Marta Family are the survivors and/or heirs of SPC Marta and are entitled to recover for the damages SPC Marta sustained.

2. The Jacob Schwallie Family

471. Sergeant Jacob Schwallie served in Afghanistan as a member of the U.S. Army. SGT Schwallie was injured in the May 7, 2012 IED Attack. SGT Schwallie died on May 7, 2012 as a result of injuries sustained during the May 7, 2012 IED Attack.

472. SGT Schwallie was a U.S. national at the time of the attack and his death.

473. Plaintiff Thomas Schwallie is the father of SGT Schwallie and a U.S. national.

474. Plaintiff Sarah Schwallie is the mother of SGT Schwallie and a U.S. national.

475. As a result of the May 7, 2012 IED Attack and SGT Schwallie's injuries and death, each member of the Schwallie Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Schwallie's society, companionship, and counsel.

476. As a result of the May 7, 2012 IED Attack, SGT Schwallie was injured in his person and/or property. The Plaintiff members of the Schwallie Family are the survivors and/or heirs of SGT Schwallie and are entitled to recover for the damages SGT Schwallie sustained.

E. May 13, 2012 Attack In Khost (Richard McNulty III Family)

477. Private First Class Richard McNulty III served in Afghanistan as a member of the U.S. Army. On May 13, 2012, PFC McNulty was injured in an IED attack in Khost. PFC McNulty died on May 13, 2012 as a result of injuries sustained during the attack.

478. The attack was committed by the Haqqani Network (a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

479. On information and belief, the bomb that the joint cell detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

480. PFC McNulty's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk, killing multiple Afghan civilians, because it occurred on a public road in front of a private hospital.

481. PFC McNulty was a U.S. national at the time of the attack and his death.

482. Plaintiff Shannon K. McNulty is the sister of PFC McNulty and a U.S. national.

483. As a result of the May 7, 2012 IED Attack and PFC McNulty's injuries and death, each member of the McNulty Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC McNulty's society, companionship, and counsel.

484. As a result of the May 13, 2012 attack, PFC McNulty was injured in his person and/or property. The Plaintiff members of the McNulty Family are the survivors and/or heirs of PFC McNulty and are entitled to recover for the damages PFC McNulty sustained.

F. May 18, 2012 Attack In Kunar (Michael Knapp Family)

485. Sergeant Michael Knapp served in Afghanistan as a member of the U.S. Army. On May 18, 2012, SGT Knapp was injured in an indirect fire attack in Kunar. SGT Knapp died that day as a result of injuries sustained during the attack.

486. The attack was committed by the the Taliban, al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

487. SGT Knapp's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and indiscriminately placed civilians at risk.

488. SGT Knapp was a U.S. national at the time of the attack and his death.

489. Plaintiff Abby Knapp-Morris is the widow of SGT Knapp and a U.S. national.

490. Plaintiff K.K., by and through her next friend Abby Knapp-Morris, is the minor daughter of SGT Knapp and a U.S. national.

491. As a result of the attack and SGT Knapp's injuries and death, each member of the Knapp Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Knapp's society, companionship, and counsel.

492. As a result of the attack, SGT Knapp was injured in his person and/or property. The Plaintiff members of the Knapp Family are the survivors and/or heirs of SGT Knapp and are entitled to recover for the damages SGT Knapp sustained.

G. May 20, 2012 Attack In Kandahar (Eric Lund Family)

493. Plaintiff Sergeant Eric Lund served in Afghanistan as a member of the U.S. Army National Guard. On May 20, 2012, SGT Lund was injured in a complex attack involving two IEDs followed by small arms fire and rocket propelled grenades in Kandahar. The attack

severely wounded SGT Lund, who lost both of his arms above the elbow, fractured his skull, broke his femur resulting in the loss of one inch of bone, broke his tibia, broke his back, and sustained a traumatic brain injury. As a result of the attack and his injuries, SGT Lund has experienced severe physical and emotional pain and suffering.

494. The attack was committed by the Taliban.

495. The attack that injured SGT Lund would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants and indiscriminately placed civilians at risk.

496. SGT Lund was a U.S. national at the time of the attack and remains so today.

H. May 20, 2012 Attack In Uruzgan (Ryan Timoney Family)

497. Plaintiff Captain Ryan Timoney served in Afghanistan as a member of the U.S. Army. On May 20, 2012, CPT Timoney was injured in a suicide bombing in Uruzgan. The attack severely wounded CPT Timoney, who lost his left leg, suffered shrapnel injuries to his left arm, left chest, left abdomen, and left side of his skull, and also suffers from spinal pain, seizures, physical limitations, and speech, reading and vision difficulty. As a result of the attack and his injuries, CPT Timoney has experienced severe physical and emotional pain and suffering.

498. The attack was committed by the Taliban and al-Qaeda (an FTO) acting together in a joint al-Qaeda-Taliban cell with al-Qaeda providing and training the suicide bomber.

499. On information and belief, the suicide bomber who detonated the bomb during the attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack

Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

500. On information and belief, the device that the suicide bomber detonated during the attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

501. The attack that injured CPT Timoney would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

502. CPT Timoney was a U.S. national at the time of the attack and remains so today.

503. Plaintiff Diane Timoney is the mother of CPT Timoney and a U.S. national.

504. Plaintiff Gregory Timoney is the father of CPT Timoney and a U.S. national.

505. As a result of the May 20, 2012 attack and CPT Timoney's injuries, each member of the Timoney Family has experienced severe mental anguish, emotional pain and suffering.

I. May 23, 2012 Attack In Kandahar (Travis Morgado Family)

506. Second Lieutenant Travis Morgado served in Afghanistan as a member of the U.S. Army. On May 23, 2012, 2LT Morgado was injured in an IED attack in Kandahar. 2LT Morgado died on May 23, 2012 as a result of injuries sustained during the attack.

507. The attack was committed by the Taliban.

508. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-

Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban’s attack.

509. 2LT Morgado’s murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

510. 2LT Morgado was a U.S. national at the time of the attack and his death.

511. Plaintiff Andrea Kessler is the mother of 2LT Morgado and a U.S. national.

512. Plaintiff Jose Morgado is the father of 2LT Morgado and a U.S. national.

513. Plaintiff Eric Morgado is the brother of 2LT Morgado and a U.S. national.

514. Plaintiff Anna Banzer is the sister of 2LT Morgado and a U.S. national.

515. Plaintiff Sofia Kessler is the sister of 2LT Morgado and a U.S. national.

516. Plaintiff Connor Pladeck-Morgado is the brother of 2LT Morgado and a U.S. national.

517. As a result of the attack and 2LT Morgado’s injuries and death, each member of the Morgado Family has experienced severe mental anguish, emotional pain and suffering, and the loss of 2LT Morgado’s society, companionship, and counsel.

518. As a result of the attack, 2LT Morgado was injured in his person and/or property. The Plaintiff members of the Morgado Family are the survivors and/or heirs of 2LT Morgado and are entitled to recover for the damages 2LT Morgado sustained.

J. May 30, 2012 Attack In Kandahar (Nicholas Olivas Family)

519. Corporal Nicholas Olivas served in Afghanistan as a member of the U.S. Army. On May 30, 2012, CPL Olivas was injured in an IED attack in Kandahar. CPL Olivas died on May 30, 2012 as a result of injuries sustained during the attack.

520. The attack was committed by the Taliban.

521. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

522. CPL Olivas's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk.

523. CPL Olivas was a U.S. national at the time of the attack and his death.

524. Plaintiff Adolf Olivas is the father of CPL Olivas and a U.S. national.

525. As a result of the May 30, 2012 attack and CPL Olivas's injuries and death, each member of the Olivas Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CPL Olivas's society, companionship, and counsel.

526. As a result of the May 30, 2012 attack, CPL Olivas was injured in his person and/or property. The Plaintiff members of the Olivas Family are the survivors and/or heirs of CPL Olivas and are entitled to recover for the damages CPL Olivas sustained.

K. May 31, 2012 Attack In Helmand (Eric Hunter Family)

527. Plaintiff Sergeant Eric Hunter served in Afghanistan as a member of the U.S. Army. On May 31, 2012, SGT Hunter was injured in an IED attack in Helmand. The attack severely wounded SGT Hunter, who lost his right leg and suffered from a severely injured left leg, post-traumatic stress disorder, and a traumatic brain injury. As a result of the attack and his injuries, SGT Hunter has experienced severe physical and emotional pain and suffering.

528. The attack was committed by the Taliban.

529. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

530. The attack that injured SGT Hunter would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk

531. SGT Hunter was a U.S. national at the time of the attack and remains so today.

532. Plaintiff Kenna Hunter is the wife of SGT Hunter and a U.S. national.

533. Plaintiff J.H., by and through his next friend Kenna Hunter, is the minor son of SGT Hunter and a U.S. national.

534. Plaintiff K.H. by and through her next friend Kenna Hunter, is the minor daughter of SGT Hunter and a U.S. national.

535. Plaintiff Betty Black is the mother of SGT Hunter and a U.S. national.

536. Plaintiff Joey Hunter Sr. is the father of SGT Hunter and a U.S. national.

537. Plaintiff Joey Hunter II is the brother of SGT Hunter and a U.S. national.

538. Plaintiff Nicholas Robinson IV is the brother of SGT Hunter and a U.S. national.

539. As a result of the May 31, 2012 attack and SGT Hunter's injuries, each member of the Hunter Family has experienced severe mental anguish, emotional pain and suffering.

L. June 12, 2012 Attack In Helmand (Erich Ellis Family)

540. Plaintiff Sergeant Erich Ellis served in Afghanistan as a member of the U.S. Marine Corps. On June 12, 2012, Sgt Ellis was injured in an IED attack in Helmand. The attack severely wounded Sgt Ellis, who lost his right leg and suffered extensive, permanent damage to his left leg, right arm, and upper right leg as well as a traumatic brain injury. As a result of the June 12, 2012 attack and his injuries, Sgt Ellis has experienced severe physical and emotional pain and suffering.

541. The attack was committed by the Taliban.

542. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

543. The attack that injured Sgt Ellis would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk.

544. Sgt Ellis was a U.S. national at the time of the attack and remains one to this day.

545. Plaintiff James Ellis is the father of Sgt Ellis and a U.S. national.

546. As a result of the June 12, 2012 attack and Sgt Ellis's injuries, each member of the Ellis Family has experienced severe mental anguish, emotional pain and suffering.

M. January 12, 2012 Attack In Kandahar (Trevor Pinnick Family)

547. Specialist Trevor Pinnick served in Afghanistan as a member of the U.S. Army. On June 12, 2012, SPC Pinnick was injured in an IED attack in Kandahar. SPC Pinnick died on June 12, 2012 as a result of injuries sustained during the attack.

548. The attack was committed by the Taliban.

549. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

550. SPC Pinnick's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

551. SPC Pinnick was a U.S. national at the time of the attack and his death.

552. Plaintiff Bethany Wesley is the sister of SPC Pinnick and a U.S. national.

553. As a result of the June 12, 2012 attack and SPC Pinnick's injuries and death, each member of the Pinnick Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Pinnick's society, companionship, and counsel.

554. As a result of the June 12, 2012 attack, SPC Pinnick was injured in his person and/or property. The Plaintiff members of the Pinnick Family are the survivors and/or heirs of SPC Pinnick and are entitled to recover for the damages SPC Pinnick sustained.

N. July 8, 2012 Attack In Wardak (Families of Cameron Stambaugh and Clarence Williams III)

555. On July 8, 2012, the Haqqani Network committed an IED attack against Americans in Wardak (“July 8, 2012, IED Attack”).

556. The July 8, 2012, IED Attack was committed by the Haqqani Network.

557. On information and belief, the bomb that the Haqqani Network detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the Haqqani Network by al-Qaeda operatives in order to facilitate the Haqqani Network’s attack.

558. The July 8, 2012, IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1. The Cameron Stambaugh Family

559. Specialist Cameron Stambaugh served in Afghanistan as a member of the U.S. Army. SPC Stambaugh was injured in the July 8, 2012, IED Attack. SPC Stambaugh died on July 8, 2012 as a result of injuries sustained during the July 8, 2012, IED Attack.

560. SPC Stambaugh was a U.S. national at the time of the attack and his death.

561. Plaintiff Mitchell L. Stambaugh is the father of SPC Stambaugh and a U.S. national.

562. As a result of the July 8, 2012, IED Attack and SPC Stambaugh's injuries and death, each member of the Stambaugh Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Stambaugh's society, companionship, and counsel.

563. As a result of the July 8, 2012, IED Attack, SPC Stambaugh was injured in his person and/or property. The Plaintiff members of the Stambaugh Family are the survivors and/or heirs of SPC Stambaugh and are entitled to recover for the damages SPC Stambaugh sustained.

2. The Clarence Williams III Family

564. Specialist Clarence Williams III served in Afghanistan as a member of the U.S. Army. SPC Williams was injured in the July 8, 2012, IED Attack. SPC Williams died on July 8, 2012 as a result of injuries sustained during the July 8, 2012, IED Attack.

565. SPC Williams was a U.S. national at the time of the attack and his death.

566. Plaintiff Clarence Williams Jr. is the father of SPC Williams and a U.S. national.

567. Plaintiff Talisa Williams is the mother of SPC Williams and a U.S. national.

568. Plaintiff Samantha Williams is the sister of SPC Williams and a U.S. national.

569. Plaintiff Abrill Williams is the sister of SPC Williams and a U.S. national.

570. As a result of the July 8, 2012 attack and SPC Williams's injuries and death, each member of the Williams Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Williams's society, companionship, and counsel.

571. As a result of the July 8, 2012 attack, SPC Williams was injured in his person and/or property. The Plaintiff members of the Williams Family are the survivors and/or heirs of SPC Williams and are entitled to recover for the damages SPC Williams sustained.

O. July 13, 2012 Attack In Zabul (Michael Ristau Family)

572. Sergeant Michael Ristau served in Afghanistan as a member of the U.S. Army. On July 13, 2012, SGT Ristau was injured in an IED attack in Zabul. SGT Ristau died on July 13, 2012 as a result of injuries sustained during the attack.

573. The attack was committed by the Haqqani Network, a part of the Taliban.

574. On information and belief, the bomb that the Haqqani Network detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Haqqani Network by al-Qaeda operatives in order to facilitate the Haqqani Network's attack.

575. SGT Ristau's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

576. SGT Ristau was a U.S. national at the time of the attack and his death.

577. Plaintiff Randy Ristau is the father of SGT Ristau and a U.S. national.

578. Plaintiff H.R., by and through her next friend Randy Ristau, is the minor sister of SGT Ristau and a U.S. national.

579. Plaintiff Suzanne Ristau is the step-mother of SGT Ristau and a U.S. national. Suzanne Ristau lived in the same household as SGT Ristau for a substantial time and considered SGT Ristau the functional equivalent of a biological son.

580. Plaintiff Christopher Powers is the step-brother of SGT Ristau and a U.S. national. Christopher Powers lived in the same household as SGT Ristau for a substantial time and considered SGT Ristau the functional equivalent of a biological brother.

581. As a result of the July 13, 2012 attack and SGT Ristau's injuries and death, each member of the Ristau Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Ristau's society, companionship, and counsel.

582. As a result of the July 13, 2012 attack, SGT Ristau was injured in his person and/or property. The Plaintiff members of the Ristau Family are the survivors and/or heirs of SGT Ristau and are entitled to recover for the damages SGT Ristau sustained.

P. July 19, 2012 Attack In Helmand (Joshua Ashley Family)

583. Sergeant Joshua Ashley served in Afghanistan as a member of the U.S. Marine Corps. On July 19, 2012, Sgt Ashley was injured in an IED attack in Helmand. Sgt Ashley died on July 19, 2012 as a result of injuries sustained during the attack.

584. The attack was committed by the Taliban.

585. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

586. Sgt Ashley's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk.

587. Sgt Ashley was a U.S. national at the time of the attack and his death.

588. Plaintiff Jonathan Ashley III is the father of Sgt Ashley and a U.S. national.

589. Plaintiff Tammie Ashley is the mother of Sgt Ashley and a U.S. national.

590. Plaintiff Jonathan Ashley IV is the brother of Sgt Ashley and a U.S. national.

591. Plaintiff Jordan Ashley is the brother of Sgt Ashley and a U.S. national.

592. As a result of the July 19, 2012 attack and Sgt Ashley's injuries and death, each member of the Ashley Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Sgt Ashley's society, companionship, and counsel.

593. As a result of the July 19, 2012 attack, Sgt Ashley was injured in his person and/or property. The Plaintiff members of the Ashley Family are the survivors and/or heirs of Sgt Ashley and are entitled to recover for the damages Sgt Ashley sustained.

Q. July 22, 2012 Attack In Logar (Justin Horsley Family)

594. Specialist Justin Horsley served in Afghanistan as a member of the U.S. Army. On July 22, 2012, SPC Horsley was injured in an IED attack in Logar. SPC Horsley died on July 22, 2012 as a result of injuries sustained during the attack.

595. The attack was committed by the Haqqani Network, a part of the Taliban.

596. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

597. SPC Horsley's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither

wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

598. SPC Horsley was a U.S. national at the time of the attack and his death.

599. Plaintiff Songmi Kietzmann is the mother of SPC Horsley and a U.S. national.

600. Plaintiff Benjamin Horsley is the brother of SPC Horsley and a U.S. national.

601. Plaintiff John Horsley is the brother of SPC Horsley and a U.S. national.

602. As a result of the July 22, 2012 attack and SPC Horsley's injuries and death, each member of the Horsley Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Horsley's society, companionship, and counsel.

603. As a result of the July 22, 2012 attack, SPC Horsley was injured in his person and/or property. The Plaintiff members of the Horsley Family are the survivors and/or heirs of SPC Horsley and are entitled to recover for the damages SPC Horsley sustained.

R. July 22, 2012 In Herat (Joseph Perez Family)

604. Mr. Joseph Perez served in Afghanistan as a civilian government contractor working for FedSys. On July 22, 2012, Mr. Perez was injured in an insider attack in Herat. Mr. Perez died on July 22, 2012 as a result of injuries sustained during the attack.

605. The attack was committed by the Taliban.

606. Mr. Perez's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, he was a civilian not taking part in hostilities, and the terrorist who committed the attack was unlawfully wearing the uniform of his enemy.

607. Mr. Perez was a U.S. national at the time of the attack and his death.

608. Plaintiff Debra Perez is the widow of Mr. Perez and a U.S. national.

609. Plaintiff Robin Akers is the daughter of Mr. Perez and a U.S. national.

610. Plaintiff Tracy Herring is the daughter of Mr. Perez and a U.S. national.

611. Plaintiff Adan Perez is the son of Mr. Perez and a U.S. national.

612. Plaintiff Anthony Perez is the son of Mr. Perez and a U.S. national.

613. Plaintiff Nicholas Perez is the son of Mr. Perez and a U.S. national.

614. As a result of the July 22, 2012 attack and Mr. Perez's injuries and death, each member of the Perez Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. Perez's society, companionship, and counsel.

615. As a result of the July 22, 2012 attack, Mr. Perez was injured in his person and/or property. The Plaintiff members of the Perez Family are the survivors and/or heirs of Mr. Perez and are entitled to recover for the damages Mr. Perez sustained.

S. August 1, 2012 Attack In Paktika (Todd Lambka Family)

616. First Lieutenant Todd Lambka served in Afghanistan as a member of the U.S. Army. On August 1, 2012, 1LT Lambka was injured in an IED attack in Paktika. 1LT Lambka died on August 1, 2012 as a result of injuries sustained during the attack.

617. The attack was committed by the Haqqani Network (a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

618. On information and belief, the bomb that the joint cell detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

619. 1LT Lambka's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither

wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk

620. 1LT Lambka was a U.S. national at the time of the attack and his death.

621. Plaintiff Brian Lambka is the father of 1LT Lambka and a U.S. national.

622. Plaintiff Jordan Lambka is the brother of 1LT Lambka and a U.S. national.

623. As a result of the August 1, 2012 attack and 1LT Lambka's injuries and death, each member of the Lambka Family has experienced severe mental anguish, emotional pain and suffering, and the loss of 1LT Lambka's society, companionship, and counsel.

624. As a result of the August 1, 2012 attack, 1LT Lambka was injured in his person and/or property. The Plaintiff members of the Lambka Family are the survivors and/or heirs of 1LT Lambka and are entitled to recover for the damages 1LT Lambka sustained.

T. August 7, 2012 Attack In Paktia (Ethan Martin Family)

625. Corporal Ethan Martin served in Afghanistan as a member of the U.S. Army. On August 7, 2012, CPL Martin was injured in an insider attack in Paktia. CPL Martin died on August 7, 2012 as a result of injuries sustained during the attack.

626. The attack was committed by the Haqqani Network (a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

627. CPL Martin's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist who committed the attack was unlawfully wearing the uniform of his enemy.

628. CPL Martin was a U.S. national at the time of the attack and his death.

629. Plaintiff Kristie Surprenant is the mother of CPL Martin and a U.S. national.

630. Plaintiff Bob Surprenant is the step-father of CPL Martin and a U.S. national. Bob Surprenant lived in the same household as CPL Martin for a substantial time and considered CPL Martin the functional equivalent of a biological son.

631. As a result of the August 7, 2012 attack and CPL Martin's injuries and death, each member of the Martin Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CPL Martin's society, companionship, and counsel.

632. As a result of the August 7, 2012 attack, CPL Martin was injured in his person and/or property. The Plaintiff members of the Martin Family are the survivors and/or heirs of CPL Martin and are entitled to recover for the damages CPL Martin sustained.

U. August 8, 2012 Attack In Kunar (Kevin Griffin Family)

633. Command Sergeant Major Kevin Griffin served in Afghanistan as a member of the U.S. Army. On August 8, 2012, CSM Griffin was injured in a suicide bombing attack in Kunar. CSM Griffin died on August 8, 2012 as a result of injuries sustained during the attack.

634. The attack was committed by the the Taliban, al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

635. On information and belief, the suicide bomber who detonated the bomb during the attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

636. On information and belief, the device that the suicide bomber detonated during the attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban

terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell’s attack.

637. CSM Griffin’s murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

638. CSM Griffin was a U.S. national at the time of the attack and his death.

639. Plaintiff Matt Griffin is the brother of CSM Griffin and a U.S. national.

640. Plaintiff Shawn Griffin is the brother of CSM Griffin and a U.S. national.

641. Plaintiff Sheila Ristaino is the sister of CSM Griffin and a U.S. national.

642. Plaintiff Daniel Griffin is the step-brother of CSM Griffin and a U.S. national.

Daniel Griffin lived in the same household as CSM Griffin for a substantial time and considered CSM Griffin the functional equivalent of a biological brother.

643. Plaintiff Carol Griffin is the step-mother of CSM Griffin and a U.S. national.

Carol Griffin lived in the same household as CSM Griffin for a substantial time and considered CSM Griffin the functional equivalent of a biological son.

644. As a result of the August 8, 2012 attack and CSM Griffin’s injuries and death, each member of the Griffin Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CSM Griffin’s society, companionship, and counsel.

645. As a result of the August 8, 2012 attack, CSM Griffin was injured in his person and/or property. The Plaintiff members of the Griffin Family are the survivors and/or heirs of CSM Griffin and are entitled to recover for the damages CSM Griffin sustained.

V. August 16, 2012 Attack In Kandahar (Richard Essex Family)

646. Sergeant Richard Essex served in Afghanistan as a member of the U.S. Army. On August 16, 2012, SGT Essex was injured in an attack on a helicopter in Kandahar. SGT Essex died on August 16, 2012 as a result of injuries sustained during the attack.

647. The attack was committed by the Taliban.

648. SGT Essex's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

649. SGT Essex was a U.S. national at the time of the attack and his death.

650. Plaintiff Charles Essex is the father of SGT Essex and a U.S. national.

651. Plaintiff Marion Hopkins is the mother of SGT Essex and a U.S. national.

652. As a result of the August 16, 2012 attack and SGT Essex's injuries and death, each member of the Essex Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Essex's society, companionship, and counsel.

653. As a result of the August 16, 2012 attack, SGT Essex was injured in his person and/or property. The Plaintiff members of the Essex Family are the survivors and/or heirs of SGT Essex and are entitled to recover for the damages SGT Essex sustained.

W. September 1, 2012 Attack In Ghazni (Families of Jeremie S. Border and Jonathan Schmidt)

654. On September 1, 2012, a joint al-Qaeda/Taliban/Lashkar-e-Taiba cell committed a complex attack involving small arms fire and grenades against Americans in Ghazni ("September 1, 2012, Complex Attack").

655. The September 1, 2012, Complex Attack was committed by the Taliban (including its Haqqani Network), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting

together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

656. The September 1, 2012, Complex Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1. The Jeremie S. Border Family

657. Staff Sergeant Jeremie Border served in Afghanistan as a member of the U.S. Army. SSG Border was injured in the September 1, 2012, Complex Attack. SSG Border died on September 1, 2012 as a result of injuries sustained during the attack.

658. SSG Border was a U.S. national at the time of the attack and his death.

659. Plaintiff Mary Border is the mother of SSG Border and a U.S. national.

660. Plaintiff Katherine Abreu-Border is the sister of SSG Border and a U.S. national.

661. Plaintiff Delaynie Peek is the sister of SSG Border and a U.S. national.

662. As a result of the September 1, 2012, Complex Attack and SSG Border's injuries and death, each member of the Border Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Border's society, companionship, and counsel.

663. As a result of the September 1, 2012 attack, SSG Border was injured in his person and/or property. The Plaintiff members of the Border Family are the survivors and/or heirs of SSG Border and are entitled to recover for the damages SSG Border sustained.

2. The Jonathan P. Schmidt Family

664. Staff Sergeant Jonathan P. Schmidt served in Afghanistan as a member of the U.S. Army. SSG Schmidt was injured in the September 1, 2012, Complex Attack. SSG Schmidt died on September 1, 2012 as a result of injuries sustained during this attack.

665. SSG Schmidt was a U.S. national at the time of the attack and his death.

666. Plaintiff Natalie Schmidt is the widow of SSG Schmidt and a U.S. national.

667. Plaintiff A.L.S., by and through his next friend Natalie Schmidt, is the minor son of SSG Schmidt and a U.S. national.

668. Plaintiff LeeAnn Schmidt is the mother of SSG Schmidt and a U.S. national.

669. Plaintiff Phillip Schmidt is the father of SSG Schmidt and a U.S. national.

670. Plaintiff Brandon Schmidt is the brother of SSG Schmidt and a U.S. national.

671. As a result of the September 1, 2012, Complex Attack and SSG Schmidt's injuries and death, each member of the Schmidt Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Schmidt's society, companionship, and counsel.

672. As a result of the September 1, 2012, Complex Attack, SSG Schmidt was injured in his person and/or property. The Plaintiff members of the Schmidt Family are the survivors and/or heirs of SSG Schmidt and are entitled to recover for the damages SSG Schmidt sustained.

X. September 13, 2012 Attack In Ghazni (Kyle Osborn Family)

673. Sergeant Kyle Osborn served in Afghanistan as a member of the U.S. Army. On September 13, 2012, SGT Osborn was injured in a rocket propelled grenade attack in Ghazni. SGT Osborn died on September 13, 2012 as a result of injuries sustained during the attack.

674. The attack was committed by the Taliban (including its Haqqani Network), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

675. SGT Osborn's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

676. SGT Osborn was a U.S. national at the time of the attack and his death.

677. Plaintiff Creighton Osborn is the father of SGT Osborn and a U.S. national.

678. Plaintiff Kade Osborn is the brother of SGT Osborn and a U.S. national.

679. Plaintiff Katlyn Osborn is the sister of SGT Osborn and a U.S. national.

680. Plaintiff Christa. Osborn is the step-mother of SGT Osborn and a U.S. national.

Christa L. Osborn lived in the same household as SGT Osborn for a substantial time and considered SGT Osborn the functional equivalent of a biological son.

681. As a result of the September 13, 2012 attack and SGT Osborn's injuries and death, each member of the Osborn Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Osborn's society, companionship, and counsel.

682. As a result of the September 13, 2012 attack, SGT Osborn was injured in his person and/or property. The Plaintiff members of the Osborn Family are the survivors and/or heirs of SGT Osborn and are entitled to recover for the damages SGT Osborn sustained.

Y. September 15, 2012 Attack In Helmand (Families of Bradley W. Atwell and Christopher K. Raible)

683. On September 15, 2012, the Taliban committed a complex attack involving small arms fire and rocket propelled grenades in Helmand ("September 15, 2012, Complex Attack").

684. The September 15, 2012, Complex Attack was committed by the Taliban.

685. The September 15, 2012, Complex Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack was unlawfully wearing the uniform of his enemy.

1. The Bradley W. Atwell Family

686. Sergeant Bradley W. Atwell served in Afghanistan as a member of the U.S. Marine Corps. Sgt Atwell was injured in the September 15, 2012, Complex Attack. Sgt Atwell died on September 15, 2012 as a result of injuries sustained during the attack.

687. SSG Border was a U.S. national at the time of the attack and his death.

688. Plaintiff Cheryl Atwell is the mother of Sgt Atwell and a U.S. national.

689. Plaintiff Erin Riedel is the sister of Sgt Atwell and a U.S. national.

690. As a result of the September 15, 2012, Complex Attack and Sgt Atwell's injuries and death, each member of the Atwell Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Border's society, companionship, and counsel.

691. As a result of the September 15, 2012, Complex Attack, Sgt Atwell was injured in his person and/or property. The Plaintiff members of the Atwell Family are the survivors and/or heirs of Sgt Atwell and are entitled to recover for the damages Sgt Atwell sustained.

2. The Christopher K. Raible Family

692. Lieutenant Colonel Christopher K. Raible served in Afghanistan as a member of the U.S. Marine Corps. LtCol Raible was injured in the September 15, 2012, Complex Attack. LtCol Raible died on September 15, 2012 as a result of injuries sustained during the attack.

693. LtCol Raible was a U.S. national at the time of the attack and his death.

694. Plaintiff Lona. Bosley is the sister of LtCol Raible and a U.S. national.

695. As a result of the attack and LtCol Raible's injuries and death, each member of the Raible Family has experienced severe mental anguish, emotional pain and suffering, and the loss of LtCol Raible's society, companionship, and counsel.

696. As a result of the attack, LtCol Raible was injured in his person and/or property. The Plaintiff members of the Raible Family are the survivors and/or heirs of LtCol Raible and are entitled to recover for the damages LtCol Raible sustained.

Z. September 16, 2012 Attack In Zabul (Jon Townsend Family)

697. Private First Class Jon Townsend served in Afghanistan as a member of the U.S. Army. On September 16, 2012, PFC Townsend was injured in an insider attack in Zabul. PFC Townsend died on September 16, 2012 as a result of injuries sustained during the attack.

698. The attack was committed by the Haqqani Network, a part of the Taliban.

699. PFC Townsend's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist who committed the attack was unlawfully wearing the uniform of his enemy.

700. PFC Townsend was a U.S. national at the time of the attack and his death.

701. Plaintiff Brittany Townsend is the widow of PFC Townsend and a U.S. national.

702. As a result of the September 16, 2012 attack and PFC Townsend's injuries and death, each member of the Townsend Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC Townsend's society, companionship, and counsel.

703. As a result of the September 16, 2012 attack, PFC Townsend was injured in his person and/or property. The Plaintiff members of the Townsend Family are the survivors and/or heirs of PFC Townsend and are entitled to recover for the damages PFC Townsend sustained.

AA. September 17, 2012 Attack In Kandahar (Kevin Trimble)

704. Plaintiff Private First Class Kevin Trimble served in Afghanistan as a member of the U.S. Army. On September 17, 2012, PFC Trimble was injured in an IED attack in Kandahar. The attack severely wounded PFC Trimble, who lost both legs above the knee, lost his left arm above the elbow, and also suffers from post-traumatic stress disorder and partial hearing loss. As

a result of the September 17, 2012 attack and his injuries, PFC Trimble has experienced severe physical and emotional pain and suffering.

705. The attack was committed by the Taliban.

706. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

707. The attack that injured PFC Trimble would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk.

708. PFC Trimble was a U.S. national at the time of the attack and remains so today.

BB. September 26, 2012 Attack In Logar (Families of Jonathan Gollnitz and Orion Sparks)

709. On September 26, 2012, a joint al-Qaeda/Taliban/Lashkar-e-Taiba cell committed a suicide bombing attack in Logar ("September 26, 2012, Suicide Attack").

710. The September 26, 2012, Suicide Attack was committed by the Taliban (including its Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

711. On information and belief, the suicide bomber who detonated the bomb during the September 26, 2012, Suicide Attack was: (i) indoctrinated by al-Qaeda regarding the purported

religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

712. On information and belief, the device that the suicide bomber detonated during the September 26, 2012, Suicide Attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

713. The September 26, 2012, Suicide Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1. The Jonathan Gollnitz Family

714. Sergeant Jonathan Gollnitz served in Afghanistan as a member of the U.S. Army. SGT Gollnitz was injured in the September 26, 2012, Suicide Attack. SGT Gollnitz died on September 26, 2012 as a result of injuries sustained during the attack.

715. SGT Gollnitz was a U.S. national at the time of the attack and his death.

716. Plaintiff L.C.D., by and through his next friend, Bridgett DeHoff, is the minor son of SGT Gollnitz and a U.S. national.

717. Plaintiff Kirk Gollnitz is the brother of SGT Gollnitz and a U.S. national.

718. Plaintiff Tyler Gollnitz is the brother of SGT Gollnitz and a U.S. national.

719. As a result of the September 26, 2012, Suicide Attack, and SGT Gollnitz's injuries and death, each member of the Gollnitz Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Gollnitz's society, companionship, and counsel.

720. As a result of the September 26, 2012, Suicide Attack, SGT Gollnitz was injured in his person and/or property. The Plaintiff members of the Gollnitz Family are the survivors and/or heirs of SGT Gollnitz and are entitled to recover for the damages SGT Gollnitz sustained.

2. The Orion Sparks Family

721. Staff Sergeant Orion Sparks served in Afghanistan as a member of the U.S. Army. SSG Sparks was injured in the September 26, 2012, Suicide Attack. SSG Sparks died on September 26, 2012 as a result of injuries sustained during the attack.

722. SSG Sparks was a U.S. national at the time of the attack and his death.

723. Plaintiff Jan Hurnblad Sparks is the mother of SSG Sparks and a U.S. national.

724. Plaintiff Garry Sparks is the father of SSG Sparks and a U.S. national.

725. Plaintiff Erik Sparks is the brother of SSG Sparks and a U.S. national.

726. Plaintiff Zachary Sparks is the brother of SSG Sparks and a U.S. national.

727. Plaintiff Jane Sparks is the step-mother of SSG Sparks and a U.S. national. Jane Sparks lived in the same household as SSG Sparks for a substantial time and considered SSG Sparks the functional equivalent of a biological son.

728. As a result of the September 26, 2012, Suicide Attack and SSG Sparks's injuries and death, each member of the Sparks Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Sparks's society, companionship, and counsel.

729. As a result of the September 26, 2012, Suicide Attack, SSG Sparks was injured in his person and/or property. The Plaintiff members of the Sparks Family are the survivors and/or heirs of SSG Sparks and are entitled to recover for the damages SSG Sparks sustained.

CC. October 1, 2012 Attack In Khost (Jeremy Hardison Family)

730. Sergeant Jeremy Hardison served in Afghanistan as a member of the U.S. Army National Guard. On October 1, 2012, SGT Hardison was injured in a suicide bombing attack by an individual wearing an Afghan police uniform in Khost. SGT Hardison died on October 1, 2012 as a result of injuries sustained during the attack.

731. The attack was committed by the Haqqani Network (a designated FTO at the time of the attack and a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

732. On information and belief, the suicide bomber who detonated the bomb during the attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

733. On information and belief, the device that the suicide bomber detonated during the attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

734. SGT Hardison's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist who committed the attack was improperly wearing the uniform of his enemy, and the attack indiscriminately placed civilians at risk, killing multiple Afghan civilians, because it occurred in a public market.

735. SGT Hardison was a U.S. national at the time of the attack and his death.

736. Plaintiff Jerry Hardison is the father of SGT Hardison and a U.S. national.

737. Plaintiff Justina Hardison is the sister of SGT Hardison and a U.S. national.

738. As a result of the October 1, 2012 attack, and SGT Hardison's injuries and death, each member of the Hardison Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Hardison's society, companionship, and counsel.

739. As a result of the October 1, 2012 attack, SGT Hardison was injured in his person and/or property. The Plaintiff members of the Hardison Family are the survivors and/or heirs of SGT Hardison and are entitled to recover for the damages SGT Hardison sustained.

DD. October 22, 2012 Attack In Kandahar (Edward Klein)

740. Plaintiff Major Edward Klein served in Afghanistan as a member of the U.S. Army. On October 22, 2012, MAJ Klein was injured in an IED attack in Kandahar. The attack severely wounded MAJ Klein, who lost both legs above the knee, his right arm, and three fingers on his left hand. As a result of the October 22, 2012 attack and his injuries, MAJ Klein has experienced severe physical and emotional pain and suffering.

741. The attack was committed by the Taliban.

742. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that

were “cooked” by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban’s attack.

743. The attack that injured MAJ Klein would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

744. MAJ Klein was a U.S. national at the time of the attack and remains so today.

745. As a result of the October 22, 2012 attack and MAJ Klein’s injuries, each member of the Klein Family has experienced severe mental anguish, emotional pain and suffering.

EE. November 3, 2012 Attack In Paktika (Ryan P. Jayne Family)

746. Specialist Ryan P. Jayne served in Afghanistan as a member of the U.S. Army Reserve. On November 3, 2012, SPC Jayne was injured in an IED attack in Paktika (“November 3, 2012 IED Attack”). SPC Jayne died on November 3, 2012 as a result of injuries sustained during the attack.

747. The November 3, 2012 IED Attack was committed by the Haqqani Network (an FTO), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

748. On information and belief, the bomb that the joint cell detonated during the November 3, 2012 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell’s attack.

749. SPC Jayne’s murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore

uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk

750. SPC Jayne was a U.S. national at the time of the attack and his death.

751. Plaintiff Paul Jayne is the father of SPC Jayne and a U.S. national.

752. Plaintiff Sherry Skeens is the mother of SPC Jayne and a U.S. national.

753. Plaintiff Adam Jayne is the brother of SPC Jayne and a U.S. national.

754. Plaintiff Ayzia Jayne is the sister of SPC Jayne and a U.S. national.

755. Plaintiff Kent Skeens is the step-father of SPC Jayne and a U.S. national. Kent Skeens lived in the same household as SPC Jayne for a substantial time and considered SPC Jayne the functional equivalent of a biological son.

756. Plaintiff Garrett Skeens is the brother of SPC Jayne and a U.S. national.

757. Plaintiff Trent Skeens is the brother of SPC Jayne and a U.S. national.

758. Plaintiff Z.S, by and through her next friend Kent Alan Skeens, is the minor sister of SPC Jayne and a U.S. national.

759. As a result of the November 3, 2012 IED Attack and SPC Jayne's injuries and death, each member of the Jayne Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Jayne's society, companionship, and counsel.

760. As a result of the November 3, 2012 IED Attack, SPC Jayne was injured in his person and/or property. The Plaintiff members of the Jayne Family are the survivors and/or heirs of SPC Jayne and are entitled to recover for the damages SPC Jayne sustained.

FF. November 16, 2012 Attack In Paktika (Joseph A. Richardson Family)

761. Sergeant Joseph Richardson served in Afghanistan as a member of the U.S. Army. On November 16, 2012, SGT Richardson was injured in a complex attack involving an

IED and small arms fire in Paktika. SGT Richardson died on November 16, 2012 as a result of injuries sustained during the attack.

762. The attack was committed by the Haqqani Network (a designated FTO at the time of the attack and a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

763. On information and belief, the bomb that the joint cell detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

764. SGT Richardson's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

765. SGT Richardson was a U.S. national at the time of the attack and his death.

766. Plaintiff Cassie Richardson is the sister of SGT Richardson and a U.S. national.

767. As a result of the November 16, 2012 attack, and SGT Richardson's injuries and death, each member of the Richardson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Richardson's society, companionship, and counsel.

768. As a result of the November 16, 2012 attack, SGT Richardson was injured in his person and/or property. The Plaintiff members of the Richardson Family are the survivors and/or heirs of SGT Richardson and are entitled to recover for the damages SGT Richardson sustained.

GG. November 18, 2012 Attack In Helmand (Dale Means Family)

769. Lance Corporal Dale Means served in Afghanistan as a member of the U.S. Marine Corps. On November 18, 2012, LCpl Means was injured in an IED attack in Helmand. LCpl Means died on November 18, 2012 as a result of injuries sustained during the attack.

770. The attack was committed by the Taliban.

771. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

772. LCpl Means's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

773. LCpl Means was a U.S. national at the time of the attack and his death.

774. Plaintiff John Means is the father of LCpl Means and a U.S. national.

775. As a result of the November 18, 2012 attack, and LCpl Means's injuries and death, each member of the Means Family has experienced severe mental anguish, emotional pain and suffering, and the loss of LCpl Means's society, companionship, and counsel.

776. As a result of the November 18, 2012 attack, LCpl Means was injured in his person and/or property. The Plaintiff members of the Means Family are the survivors and/or heirs of LCpl Means and are entitled to recover for the damages LCpl Means sustained.

HH. December 15, 2012 Attack In Kabul (Mark Schoonhoven Family)

777. Staff Sergeant Mark Schoonhoven served in Afghanistan as a member of the U.S. Army. On December 15, 2012, SSG Schoonhoven was injured in an IED attack in Kabul. SSG Schoonhoven died on January 20, 2013 as a result of injuries sustained during the attack.

778. The attack was committed by the Taliban (including its Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

779. The attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Kabul Attack Network's funding, logistics, personnel, and weapons supply in his capacity as a member of al-Qaeda's military council, and helped choose the general time and target for the attack.

780. On information and belief, the bomb that the joint cell detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

781. SSG Schoonhoven's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk.

782. SSG Schoonhoven was a U.S. national at the time of the attack and his death.

783. Plaintiff Tammie Schoonhoven is the widow of SSG Schoonhoven and a U.S. national.

784. Plaintiff A.M.S., by and through her next friend Tammie Schoonhoven, is the minor daughter of SSG Schoonhoven and a U.S. national.

785. Plaintiff A.R.S., by and through her next friend Tammie Schoonhoven, is the minor daughter of SSG Schoonhoven and a U.S. national.

786. Plaintiff Deborah Schoonhoven is the mother of SSG Schoonhoven and a U.S. national.

787. Plaintiff Christopher Schoonhoven is the brother of SSG Schoonhoven and a U.S. national.

788. Plaintiff Sheeshta Perry is the step-daughter of SSG Schoonhoven and a U.S. national. Ms. Perry lived in the same household as SSG Schoonhoven for a substantial period and considered SSG Schoonhoven the functional equivalent of a biological father.

789. As a result of the December 15, 2012 attack, and SSG Schoonhoven's injuries and death, each member of the Schoonhoven Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Schoonhoven's society, companionship, and counsel.

790. As a result of the December 15, 2012 attack, SSG Schoonhoven was injured in his person and/or property. The Plaintiff members of the Schoonhoven Family are the survivors and/or heirs of SSG Schoonhoven and are entitled to recover for the damages SSG Schoonhoven sustained.

II. February 22, 2013 Attack In Helmand (Jonathan D. Davis Family)

791. Staff Sergeant Jonathan D. Davis served in Afghanistan as a member of the U.S. Marine Corps. On February 22, 2013, SSgt Davis was injured in an IED attack in Helmand. SSgt Davis died on February 22, 2013 as a result of injuries sustained during the attack.

792. The attack was committed by the Taliban.

793. On information and belief, the bomb that the Taliban detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

794. SSgt Davis's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

795. SSgt Davis was a U.S. national at the time of the attack and his death.

796. Plaintiff Helena Davis is the widow of SSgt Davis and a U.S. national.

797. Plaintiff C.D., by and through his next friend Helena Davis, is the minor son of SSgt Davis and a U.S. national.

798. As a result of the February 22, 2013 attack, and SSgt Davis's injuries and death, each member of the Davis Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSgt Davis's society, companionship, and counsel.

799. As a result of the February 22, 2013 attack, SSgt Davis was injured in his person and/or property. The Plaintiff members of the Davis Family are the survivors and/or heirs of SSgt Davis and are entitled to recover for the damages SSgt Davis sustained.

JJ. March 11, 2013 Attack In Wardak (Rex L. Schad Family)

800. Staff Sergeant Rex Schad served in Afghanistan as a member of the U.S. Army. On March 11, 2013, SSG Schad was injured in an insider attack in Wardak. SSG Schad died on March 11, 2013 as a result of injuries sustained during the attack.

801. The attack was committed by the Haqqani Network, a part of the Taliban.

802. SSG Schad's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist who committed the attack was unlawfully wearing the uniform of his enemy.

803. SSG Schad was a U.S. national at the time of the attack and his death.

804. Plaintiff Colleen Whipple is the mother of SSG Schad and a U.S. national.

805. As a result of the March 11, 2013 attack, and SSG Schad's injuries and death, each member of the Schad Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Schad's society, companionship, and counsel.

806. As a result of the March 11, 2013 attack, SSG Schad was injured in his person and/or property. The Plaintiff members of the Schad Family are the survivors and/or heirs of SSG Schad and are entitled to recover for the damages SSG Schad sustained.

KK. April 6, 2013 Attack In Zabul (Anne T. Smedinghoff Family)

807. Ms. Anne T. Smedinghoff served in Afghanistan as a U.S. Foreign Service Officer working for the U.S. Department of State. On April 6, 2013, Ms. Smedinghoff was injured in a suicide bombing attack in Zabul. Ms. Smedinghoff died on April 6, 2013 as a result of injuries sustained during the attack.

808. The attack was committed by the Taliban (including the Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell in the Kabul Attack Network.

809. On information and belief, the suicide bomber who detonated the bomb during the attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

810. On information and belief, the device that the suicide bomber detonated during the attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

811. Ms. Smedinghoff's murder would have violated the laws of war if these terrorists were subject to them because, among other reasons, she was a civilian State Department Employee not taking part in hostilities and escorting Afghan journalists covering American officials donating books to a school.

812. Ms. Smedinghoff was a U.S. national at the time of the attack and her death.

813. Plaintiff Mary Smedinghoff is the mother of Ms. Smedinghoff and a U.S. national.

814. Plaintiff Thomas Smedinghoff is the father of Ms. Smedinghoff and a U.S. national.

815. Plaintiff Joan Smedinghoff is the sister of Ms. Smedinghoff and a U.S. national.

816. Plaintiff Mark Smedinghoff is the brother of Ms. Smedinghoff and a U.S. national.

817. Plaintiff Regina Smedinghoff is the sister of Ms. Smedinghoff and a U.S. national.

818. As a result of the March 11, 2013 attack, and Ms. Smedinghoff's injuries and death, each member of the Smedinghoff Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Ms. Smedinghoff's society, companionship, and counsel.

819. As a result of the April 6, 2013 attack, Ms. Smedinghoff was injured in her person and/or property. The Plaintiff members of the Smedinghoff Family are the survivors and/or heirs of Ms. Smedinghoff and are entitled to recover for the damages Ms. Smedinghoff sustained.

LL. May 4, 2013 Attack In Kandahar (Families of Kevin Cardoza, Brandon J. Landrum, Thomas P. Murach, Francis G. Phillips IV, and Brandon J. Prescott)

820. On May 4, 2013, the Taliban committed an IED attack targeting Americans in Kandahar ("May 4, 2013 IED Attack").

821. On information and belief, the bomb that the Taliban detonated during the May 4, 2013 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

822. The May 4, 2013 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Kevin Cardoza Family

823. Specialist Kevin Cardoza served in Afghanistan as a member of the U.S. Army. SPC Cardoza was injured in the May 4, 2013 IED Attack. SPC Cardoza died on May 4, 2013 as a result of injuries sustained during the May 4, 2013 IED Attack.

824. SPC Cardoza was a U.S. national at the time of the attack and his death.

825. Plaintiff Maria Cardoza is the mother of SPC Cardoza and a U.S. national.

826. Plaintiff Ramiro Cardoza Sr. is the father of SPC Cardoza and a U.S. national.

827. Plaintiff Ramiro Cardoza Jr. is the brother of SPC Cardoza and a U.S. national.

828. As a result of the May 4, 2013 Attack, and SPC Cardoza's injuries and death, each member of the Cardoza Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Cardoza's society, companionship, and counsel.

829. As a result of the May 4, 2013 Attack, SPC Cardoza was injured in his person and/or property. The Plaintiff members of the Cardoza Family are the survivors and/or heirs of SPC Cardoza and are entitled to recover for the damages SPC Cardoza sustained.

2. The Brandon J. Landrum Family

830. First Lieutenant Brandon J. Landrum served in Afghanistan as a member of the U.S. Army. 1LT Landrum was injured in the May 4, 2013 IED Attack. 1LT Landrum died on May 4, 2013 as a result of injuries sustained during the May 4, 2013 IED Attack.

831. 1LT Landrum was a U.S. national at the time of the attack and his death.

832. Plaintiff Miranda Landrum is the widow of 1LT Landrum and a U.S. national.

833. Plaintiff B.R.L., by and through her next friend Miranda Landrum, is the minor daughter of 1LT Landrum and a U.S. national.

834. Plaintiff G.B.L., by and through his next friend Miranda Landrum, is the minor son of 1LT Landrum and a U.S. national.

835. Plaintiff Janet Landrum is the mother of 1LT Landrum and a U.S. national

836. Plaintiff James Landrum is the father of 1LT Landrum and a U.S. national.

837. As a result of the May 4, 2013 Attack, and 1LT Landrum's injuries and death, each member of the Landrum Family has experienced severe mental anguish, emotional pain and suffering, and the loss of 1LT Landrum's society, companionship, and counsel.

838. As a result of the May 4, 2013 Attack, 1LT Landrum was injured in his person and/or property. The Plaintiff members of the Landrum Family are the survivors and/or heirs of 1LT Landrum and are entitled to recover for the damages 1LT Landrum sustained.

3. The Thomas P. Murach Family

839. Specialist Thomas Paige Murach served in Afghanistan as a member of the U.S. Army. SPC Murach was injured in the May 4, 2013 IED Attack. SPC Murach died on May 4, 2013 as a result of injuries sustained during the May 4, 2013 IED Attack.

840. SPC Murach was a U.S. national at the time of the May 4, 2013 IED Attack and his death.

841. Plaintiff Chet Murach is the father of SPC Murach and a U.S. national.

842. Plaintiff William Murach is the brother of SPC Murach and a U.S. national.

843. As a result of the May 4, 2013 Attack, and SPC Murach's injuries and death, each member of the Murach Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Murach's society, companionship, and counsel.

844. As a result of the May 4, 2013 Attack, SPC Murach was injured in his person and/or property. The Plaintiff members of the Murach Family are the survivors and/or heirs of SPC Murach and are entitled to recover for the damages SPC Murach sustained.

4. The Francis G. Phillips IV Family

845. Staff Sergeant Francis G. Phillips IV served in Afghanistan as a member of the U.S. Army. SSG Phillips was injured in the May 4, 2013 IED Attack. SSG Phillips died on May 4, 2013 as a result of injuries sustained during the May 4, 2013 IED Attack.

846. SSG Phillips was a U.S. national at the time of the May 4, 2013 IED Attack and his death.

847. Plaintiff Christine H. Phillips is the widow of SSG Phillips and a U.S. national.

848. Plaintiff S.N.P., by and through her next friend Christine H. Phillips, is the minor daughter of SSG Phillips and a U.S. national.

849. As a result of the May 4, 2013 Attack, and SSG Phillips's injuries and death, each member of the Phillips Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Phillips's society, companionship, and counsel.

850. As a result of the May 4, 2013 Attack, SSG Phillips was injured in his person and/or property. The Plaintiff members of the Phillips Family are the survivors and/or heirs of SSG Phillips and are entitled to recover for the damages SSG Phillips sustained.

5. The Brandon J. Prescott Family

851. Specialist Brandon J. Prescott served in Afghanistan as a member of the U.S. Army. SPC Prescott was injured in the May 4, 2013 IED Attack. SPC Prescott died on May 4, 2013 as a result of injuries sustained during the May 4, 2013 IED Attack.

852. SPC Prescott was a U.S. national at the time of the May 4, 2013 IED Attack and his death.

853. Plaintiff Tracey Prescott is the mother of SPC Prescott and a U.S. national.

854. Plaintiff Aaron Prescott is the brother of SPC Prescott and a U.S. national.

855. Plaintiff Jacob Prescott is the brother of SPC Prescott and a U.S. national.

856. Plaintiff Joshua Prescott is the brother of SPC Prescott and a U.S. national.

857. As a result of the May 4, 2013 Attack, and SPC Prescott's injuries and death, each member of the Prescott Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Prescott's society, companionship, and counsel.

858. As a result of the May 4, 2013 Attack, SPC Prescott was injured in his person and/or property. The Plaintiff members of the Prescott Family are the survivors and/or heirs of SPC Prescott and are entitled to recover for the damages SPC Prescott sustained.

MM. May 14, 2013 Attack In Kandahar (Families of Mitchell Daehling and William J. Gilbert)

859. On May 14, 2013, the Taliban committed an IED attack targeting Americans in Kandahar ("May 14, 2013 IED Attack").

860. On information and belief, the bomb that the Taliban detonated during the May 14, 2013 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

861. The May 14, 2013 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Mitchell Daehling Family

862. Specialist Mitchell Daehling served in Afghanistan as a member of the U.S. Army. SPC Daehling was injured in the May 14, 2013 IED Attack. SPC Daehling died on May 14, 2013 as a result of injuries sustained during the May 14, 2013 IED Attack.

863. SPC Daehling was a U.S. national at the time of the May 14, 2013 IED Attack and his death.

864. Plaintiff Samantha McNamara is the widow of SPC Daehling and a U.S. national.

865. Plaintiff Brenda Daehling is the mother of SPC Daehling and a U.S. national.

866. Plaintiff Kirk Daehling is the father of SPC Daehling and a U.S. national.

867. Plaintiff Adam Daehling is the brother of SPC Daehling and a U.S. national.

868. Plaintiff Kayla Daehling is the sister of SPC Daehling and a U.S. national.

869. As a result of the May 14, 2013 Attack, and SPC Daehling's injuries and death, each member of the Daehling Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Daehling's society, companionship, and counsel.

870. As a result of the May 14, 2013 IED Attack, SPC Daehling was injured in his person and/or property. The Plaintiff members of the Daehling Family are the survivors and/or heirs of SPC Daehling and are entitled to recover for the damages SPC Daehling sustained.

2. The William J. Gilbert Family

871. Specialist William J. Gilbert served in Afghanistan as a member of the U.S. Army. SPC Gilbert was injured in the May 14, 2013 IED Attack. SPC Gilbert died on May 14, 2013 as a result of injuries sustained during the May 14, 2013 IED Attack.

872. SPC Gilbert was a U.S. national at the time of the May 14, 2013 IED Attack and his death.

873. Plaintiff Joanna Gilbert is the mother of SPC Gilbert and a U.S. national.

874. Plaintiff Jessica Benson is the sister of SPC Gilbert and a U.S. national.

875. As a result of the May 14, 2013 Attack, and SPC Gilbert's injuries and death, each member of the Gilbert Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Gilbert's society, companionship, and counsel.

876. As a result of the May 14, 2013 IED Attack, SPC Gilbert was injured in his person and/or property. The Plaintiff members of the Gilbert Family are the survivors and/or heirs of SPC Gilbert and are entitled to recover for the damages SPC Gilbert sustained.

NN. May 16, 2013 Attack In Kabul (Angel Roldan Jr. Family)

877. Mr. Angel Roldan Jr. served in Afghanistan as a civilian government contractor working for DynCorp, Int'l. On May 16, 2013, Mr. Roldan was injured in a suicide bombing attack in Kabul ("May 16, 2013 Suicide Attack"). Mr. Roldan died on May 16, 2013 as a result of injuries sustained during the May 16, 2013 Suicide Attack.

878. The May 16, 2013 Suicide Attack was committed by the Taliban (including its Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

879. The May 16, 2013 Suicide Attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Kabul Attack Network's funding, logistics, personnel, and weapons supply in his capacity as a member of al-Qaeda's military council, and helped choose the general time and target for the May 16, 2013 Suicide Attack.

880. On information and belief, the suicide bomber who detonated the bomb during the May 16, 2013 Suicide Attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's

tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

881. On information and belief, the device that the suicide bomber detonated during the May 16, 2013 Suicide Attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

882. The May 16, 2013 Suicide Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, Mr. Roldan was a civilian not taking part in hostilities, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk, killing multiple Afghan civilians, because it occurred on a public road during rush hour.

883. Mr. Roldan was a U.S. national at the time of the May 16, 2013 Suicide Attack and his death.

884. Plaintiff Lieselotte Roldan is the widow of Mr. Roldan and a U.S. national.

885. Plaintiff Angel Roldan is the son of Mr. Roldan and a U.S. national.

886. Plaintiff Matthias Roldan is the son of Mr. Roldan and a U.S. national.

887. Plaintiff Samantha Roldan is the daughter of Mr. Roldan and a U.S. national.

888. As a result of the May 16, 2013 Suicide Attack, and SPC Gilbert's injuries and death, each member of the Roldan Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. Roldan's society, companionship, and counsel.

889. As a result of the May 16, 2013 Suicide Attack, Mr. Roldan was injured in his person and/or property. The Plaintiff members of the Roldan Family are the survivors and/or heirs of Mr. Roldan and are entitled to recover for the damages Mr. Roldan sustained.

OO. June 2, 2013 Attack In Helmand (Sean W. Mullen Family)

890. Warrant Officer Sean W. Mullen served in Afghanistan as a member of the U.S. Army. On June 2, 2013, WO1 Mullen was injured in an IED attack in Helmand ("June 2, 2013 IED Attack"). WO1 Mullen died on June 2, 2013 as a result of injuries sustained during the June 2, 2013 IED Attack.

891. The June 2, 2013 IED Attack was committed by the Taliban.

892. On information and belief, the bomb that the Taliban detonated during the June 2, 2013 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

893. The June 2, 2013 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

894. WO1 Mullen was a U.S. national at the time of the June 2, 2013 IED Attack and his death.

895. Plaintiff Nancy Mullen is the widow of WO1 Mullen and a U.S. national.

896. Plaintiff Miriam Mullen is the mother of WO1 Mullen and a U.S. national.

897. Plaintiff William Mullen is the father of WO1 Mullen and a U.S. national.

898. As a result of the June 2, 2013 IED Attack, and WO1 Mullen's injuries and death, each member of the Mullen Family has experienced severe mental anguish, emotional pain and suffering, and the loss of WO1 Mullen's society, companionship, and counsel.

899. As a result of the June 2, 2013 IED Attack, WO1 Mullen was injured in his person and/or property. The Plaintiff members of the Mullen Family are the survivors and/or heirs of WO1 Mullen and are entitled to recover for the damages WO1 Mullen sustained.

PP. June 18, 2013 Attack In Parwan (Robert W. Ellis Family)

900. Specialist Robert W. Ellis served in Afghanistan as a member of the U.S. Army. On June 18, 2013, SPC Ellis was injured in a rocket attack in Parwan ("June 18, 2013 Rocket Attack"). SPC Ellis died on June 18, 2013 as a result of injuries sustained during the June 18, 2013 Rocket Attack.

901. The June 18, 2013 Rocket Attack was committed by the Taliban.

902. The June 18, 2013 Rocket Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

903. SPC Ellis was a U.S. national at the time of the June 18, 2013 Rocket Attack and his death.

904. Plaintiff Joelle Ellis is the mother of SPC Ellis and a U.S. national.

905. Plaintiff John Ellis is the father of SPC Ellis and a U.S. national.

906. Plaintiff James Ellis is the brother of SPC Ellis and a U.S. national.

907. As a result of the June 18, 2013 Rocket Attack, and SPC Ellis's injuries and death, each member of the Ellis Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Ellis's society, companionship, and counsel.

908. As a result of the June 18, 2013 attack, SPC Ellis was injured in his person and/or property. The Plaintiff members of the Ellis Family are the survivors and/or heirs of SPC Ellis and are entitled to recover for the damages SPC Ellis sustained.

QQ. June 23, 2013 Attack In Paktika (Brandon Korona)

909. Plaintiff Sergeant Brandon Korona served in Afghanistan as a member of the U.S. Army. On June 23, 2013, SGT Korona was injured in an IED attack in Paktika. The attack severely wounded SGT Korona, who suffered from significant injuries to his left leg requiring a below-knee amputation in 2017, a fractured right ankle, and a traumatic brain injury. As a result of the June 23, 2013 attack and his injuries, SGT Korona has experienced severe physical and emotional pain and suffering.

910. The attack was committed by the Haqqani Network (a designated FTO at the time of the attack and a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

911. On information and belief, the bomb that the joint cell detonated during the attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

912. The attack that injured SGT Korona would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

913. SGT Korona was a U.S. national at the time of the attack and remains so today.

RR. July 15, 2013 Attack In Paktika (Sonny C. Zimmerman Family)

914. Staff Sergeant Sonny Zimmerman served in Afghanistan as a member of the U.S. Army. On July 15, 2013, SSG Zimmerman was injured in an attack involving a recoilless rifle in Paktia (“July 15, 2013 Recoilless Rifle Attack”). SSG Zimmerman died on July 16, 2013 as a result of injuries sustained during the July 15, 2013 Recoilless Rifle Attack.

915. The July 15, 2013 Recoilless Rifle Attack was committed by the Haqqani Network (a designated FTO at the time of the attack and a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

916. The July 15, 2013 Recoilless Rifle Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

917. SSG Zimmerman was a U.S. national at the time of the July 15, 2013 Recoilless Rifle Attack and his death.

918. Plaintiff Michelle Zimmerman is the mother of SSG Zimmerman and a U.S. national.

919. Plaintiff Chris Zimmerman is the father of SSG Zimmerman and a U.S. national.

920. Plaintiff Baily Zimmerman is the sister of SSG Zimmerman and a U.S. national.

921. As a result of the July 15, 2013 Recoilless Rifle Attack, and SSG Zimmerman’s injuries and death, each member of the Zimmerman Family has experienced severe mental

anguish, emotional pain and suffering, and the loss of SSG Zimmerman's society, companionship, and counsel.

922. As a result of the July 15, 2013 Recoilless Rifle Attack, SSG Zimmerman was injured in his person and/or property. The Plaintiff members of the Zimmerman Family are the survivors and/or heirs of SSG Zimmerman and are entitled to recover for the damages SSG Zimmerman sustained.

SS. July 23, 2013 Attack In Wardak (Families of Rob L. Nichols and Nickolas S. Welch)

923. On July 23, 2013, the Haqqani Network (an FTO at the time and part of the Taliban) committed an IED attack targeting Americans in Wardak ("July 23, 2013 IED Attack").

924. On information and belief, the bomb that the Taliban detonated during the July 23, 2013 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

925. The July 23, 2013 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Rob L. Nichols Family

926. Specialist Rob L. Nichols served in Afghanistan as a member of the U.S. Army. SPC Nichols was injured in the July 23, 2013 IED Attack. SPC Nichols died on July 23, 2013 as a result of injuries sustained during the July 23, 2013 IED Attack.

927. SPC Nichols was a U.S. national at the time of the July 23, 2013 IED Attack and his death.

928. Plaintiff Bruce Nichols is the father of SPC Nichols and a U.S. national.

929. Plaintiff M.G.N., by and through her next friend Bruce Nichols, is the minor sister of SPC Nichols and a U.S. national.

930. Plaintiff Jeanne Nichols is the step-mother of SPC Nichols and a U.S. national. Jeanne Nichols lived in the same household as SPC Nichols for a substantial time and considered SPC Nichols the functional equivalent of a biological son.

931. As a result of the July 23, 2013 IED Attack, and SPC Nichols's injuries and death, each member of the Nichols Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Nichols's society, companionship, and counsel.

932. As a result of the July 23, 2013 IED Attack, SPC Nichols was injured in his person and/or property. The Plaintiff members of the Nichols Family are the survivors and/or heirs of SPC Nichols and are entitled to recover for the damages SPC Nichols sustained.

2. The Nickolas S. Welch Family

933. Specialist Nickolas S. Welch served in Afghanistan as a member of the U.S. Army. SPC Nichols was injured in the July 23, 2013 IED Attack. SPC Welch died two weeks later, on August 6, 2013, as a result of injuries sustained during the July 23, 2013 IED Attack.

934. SPC Welch was a U.S. national at the time of the July 23, 2013 IED Attack and his death.

935. Plaintiff Lorria Welch is the mother of SPC Welch and a U.S. national.

936. Plaintiff Barry Welch is the father of SPC Welch and a U.S. national.

937. Plaintiff Zackary Welch is the brother of SPC Welch and a U.S. national.

938. As a result of the July 23, 2013 IED Attack, and SPC Welch's injuries and death, each member of the Welch Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Welch's society, companionship, and counsel.

939. As a result of the July 23, 2013 IED Attack, SPC Welch was injured in his person and/or property. The Plaintiff members of the Welch Family are the survivors and/or heirs of SPC Welch and are entitled to recover for the damages SPC Welch sustained.

TT. July 30, 2013 Attack In Logar (Nicholas B. Burley Family)

940. Specialist Nicholas B. Burley served in Afghanistan as a member of the U.S. Army. On July 30, 2013, SPC Burley was injured in an indirect fire attack in Logar ("July 30, 2013 Indirect Fire Attack"). SPC Burley died on July 30, 2013 as a result of injuries sustained during the July 30, 2013 Indirect Fire Attack.

941. The July 30, 2013 Indirect Fire Attack was committed by the Haqqani Network, a designated FTO at the time of the attack and part of the Taliban.

942. The July 30, 2013 Indirect Fire Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and indiscriminately placed civilians at risk.

943. SPC Burley was a U.S. national at the time of the July 30, 2013 Indirect Fire Attack and his death.

944. Plaintiff Tammy Olmstead is the mother of SPC Burley and a U.S. national.

945. Plaintiff William M. Burley is the father of SPC Burley and a U.S. national.

946. Plaintiff Michael Collins is the brother of SPC Burley and a U.S. national.

947. Plaintiff Dan Olmstead is the step-father of SPC Burley and a U.S. national. Dan Olmstead lived in the same household as SPC Burley for a substantial time and considered SPC Burley the functional equivalent of a biological son.

948. As a result of the July 30, 2013 Indirect Fire Attack, and SPC Burley's injuries and death, each member of the Burley Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Burley's society, companionship, and counsel.

949. As a result of the July 30, 2013 Indirect Fire Attack, SPC Burley was injured in his person and/or property. The Plaintiff members of the Burley Family are the survivors and/or heirs of SPC Burley and are entitled to recover for the damages SPC Burley sustained.

UU. August 12, 2013 Attack In Logar (James T. Wickliff Chacin Family)

950. Specialist James Wickliff Chacin served in Afghanistan as a member of the U.S. Army. On August 12, 2013, SPC Wickliff Chacin was injured in an IED attack in Logar ("August 12, 2013 IED Attack"). SPC Wickliff Chacin died 38 days later, on September 20, 2013, as a result of injuries sustained during the August 12, 2013 IED Attack.

951. The August 12, 2013 IED Attack was committed by the Haqqani Network, a designated FTO at the time of the attack and part of the Taliban.

952. On information and belief, the bomb that the joint cell detonated during the August 12, 2013 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

953. The August 12, 2013 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the

IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

954. SPC Wickliff Chacin was a U.S. national at the time of the August 12, 2013 IED Attack and his death.

955. Plaintiff Martha Smith is the mother of SPC Wickliff Chacin and a U.S. national.

956. Plaintiff Thomas Wickliff is the father of SPC Wickliff Chacin and a U.S. national.

957. Plaintiff Michelle Rotelli is the sister of SPC Wickliff Chacin and a U.S. national.

958. As a result of the August 12, 2013 IED Attack, and SPC Wickliff Chacin's injuries and death, each member of the Wickliff Chacin Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Wickliff-Chacin's society, companionship, and counsel.

959. As a result of the August 12, 2013 IED Attack, SPC Wickliff Chacin was injured in his person and/or property. The Plaintiff members of the Wickliff Chacin Family are the survivors and/or heirs of SPC Wickliff Chacin and are entitled to recover for the damages SPC Wickliff Chacin sustained.

VV. September 21, 2013 Attack In Paktia (Families of Liam Nevins and Joshua J. Strickland)

960. On September 21, 2013, the Haqqani Network (an FTO at the time and part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell committed an insider attack targeting Americans in Paktia ("September 21, 2013 Insider Attack").

961. The September 21, 2013 Insider Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack was lawfully wearing the uniform of his enemy.

1. The Liam Nevins Family

962. Sergeant First Class Liam Nevins served in Afghanistan as a member of the U.S. Army. SFC Nevins was injured in the September 21, 2013 Insider Attack. SFC Nevins died on September 21, 2013 as a result of injuries sustained during this attack.

963. SFC Nevins was a U.S. national at the time of the September 21, 2013 Insider Attack and his death.

964. Plaintiff William Nevins is the father of SFC Nevins and a U.S. national.

965. As a result of the September 21, 2013 Insider Attack, and SFC Nevins's injuries and death, each member of the Nevins Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SFC Nevins's society, companionship, and counsel.

966. As a result of the September 21, 2013 Insider Attack, SFC Nevins was injured in his person and/or property. The Plaintiff members of the Nevins Family are the survivors and/or heirs of SFC Nevins and are entitled to recover for the damages SFC Nevins sustained.

2. The Joshua J. Strickland Family

967. Sergeant Joshua Strickland served in Afghanistan as a member of the U.S. Army. SGT Strickland was injured in the September 21, 2013 Insider Attack. SGT Strickland died on September 21, 2013 as a result of injuries sustained during the attack.

968. SGT Strickland was a U.S. national at the time of the September 21, 2013 Insider Attack and his death.

969. Plaintiff Garrett Funk is the brother of SGT Strickland and a U.S. national.

970. As a result of the September 21, 2013 Insider Attack, and SGT Strickland's injuries and death, each member of the Strickland Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Strickland's society, companionship, and counsel.

971. As a result of the September 21, 2013 Insider Attack, SGT Strickland was injured in his person and/or property. The Plaintiff members of the Strickland Family are the survivors and/or heirs of SGT Strickland and are entitled to recover for the damages SGT Strickland sustained.

WW. September 26, 2013 Attack In Paktia (Thomas A. Baysore Jr. Family)

972. Staff Sergeant Thomas Baysore Jr. served in Afghanistan as a member of the U.S. Army. On September 26, 2013, SSG Baysore was injured in an insider attack in Paktia ("September 26, 2013 Insider Attack"). SSG Baysore died on September 26, 2013 as a result of injuries sustained during the September 26, 2013 Insider Attack.

973. The September 26, 2013 Insider Attack was committed by the Haqqani Network (a designated FTO at the time of the attack and a part of the Taliban), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together in a joint cell.

974. The September 26, 2013 Insider Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack was unlawfully wearing the uniform of his enemy.

975. SSG Baysore was a U.S. national at the time of the September 26, 2013 Insider Attack and his death.

976. Plaintiff Angela Kahler is the sister of SSG Baysore and a U.S. national.

977. As a result of the September 26, 2013 Insider Attack, and SSG Baysore's injuries and death, each member of the Baysore Family has experienced severe mental anguish,

emotional pain and suffering, and the loss of SSG Baysore's society, companionship, and counsel.

978. As a result of the September 26, 2013 Insider Attack, SSG Baysore was injured in his person and/or property. The Plaintiff members of the Baysore Family are the survivors and/or heirs of SSG Baysore and are entitled to recover for the damages SSG Baysore sustained.

XX. October 6, 2013 Attack In Kandahar (Families of Cody Patterson and Joseph M. Peters)

979. On October 6, 2013, the Taliban committed an IED targeting Americans in Kandahar ("October 6, 2013 IED Attack").

980. On information and belief, the bomb that the Taliban detonated during the October 6, 2013 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

981. The October 6, 2013 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Cody Patterson Family

982. Specialist Cody Patterson served in Afghanistan as a member of the U.S. Army. SPC Patterson was injured in the October 6, 2013 IED Attack. SPC Patterson died on October 6, 2013 as a result of injuries sustained during the October 6, 2013 IED Attack.

983. SPC Patterson was a U.S. national at the time of the October 6, 2013 IED Attack and his death.

984. Plaintiff Nancy Wilson is the mother of SPC Patterson and a U.S. national.

985. As a result of the October 6, 2013 IED Attack, and SPC Patterson's injuries and death, each member of the Patterson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Patterson's society, companionship, and counsel.

986. As a result of the October 6, 2013 IED Attack, SPC Patterson was injured in his person and/or property. The Plaintiff members of the Patterson Family are the survivors and/or heirs of SPC Patterson and are entitled to recover for the damages SPC Patterson sustained.

2. The Joseph M. Peters Family

987. Sergeant Joseph Peters served in Afghanistan as a member of the U.S. Army. SGT Peters was injured in the October 6, 2013 IED Attack. SGT Peters died on October 6, 2013 as a result of injuries sustained during the October 6, 2013 IED Attack.

988. SGT Peters was a U.S. national at the time of the October 6, 2013 IED Attack and his death.

989. Plaintiff Ashley Peters is the widow of SGT Peters and a U.S. national.

990. Plaintiff G.R.P., by and through his next friend Ashley Peters, is the minor son of SGT Peters and a U.S. national.

991. Plaintiff Deborah Peters is the mother of SGT Peters and a U.S. national.

992. Plaintiff Dennis Peters is the father of SGT Peters and a U.S. national.

993. As a result of the October 6, 2013 IED Attack, and SGT Peters's injuries and death, each member of the Peters Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Peters's society, companionship, and counsel.

994. As a result of the October 6, 2013 IED Attack, SGT Peters was injured in his person and/or property. The Plaintiff members of the Peters Family are the survivors and/or heirs of SGT Peters and are entitled to recover for the damages SGT Peters sustained.

YY. February 10, 2014 Attack In Kabul (Families Of Paul Goins Jr. And Michael A. Hughes)

995. On February 10, 2014, a joint cell comprised of the Taliban (including its Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO), led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, and acting together as part of the Kabul Attack Network, committed an IED attack targeting Americans in Kabul (“February 10, 2014 IED Attack”).

996. The February 10, 2014 IED Attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Kabul Attack Network’s funding, logistics, personnel, and weapons supply in his capacity as a member of al-Qaeda’s military council, and helped choose the general time and target for the attack.

997. On information and belief, the bomb that the joint cell detonated during the February 10, 2014 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell’s attack.

998. The February 10, 2014 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorists targeted civilians not taking part in hostilities, the terrorist(s) who planted the IED neither wore uniforms nor

otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1. The Paul Goins Jr. Family

999. Mr. Paul Goins Jr. served in Afghanistan as a civilian government contractor working for DynCorp, Int'l. Mr. Goins was injured in the February 10, 2014 IED Attack. Mr. Goins died on February 10, 2014 as a result of injuries sustained during the attack.

1000. Mr. Goins was a U.S. national at the time of the February 10, 2014 IED Attack and his death.

1001. Plaintiff Patricia Goins is the widow of Mr. Goins and a U.S. national.

1002. Plaintiff Paul E. Goins III is the son of Mr. Goins and a U.S. national.

1003. Plaintiff Emmitt Burns is the step-son of Mr. Goins and a U.S. national. Emmitt Dwayne Burns lived in the same household as Mr. Goins for a substantial time and considered Mr. Goins the functional equivalent of a biological father.

1004. Plaintiff Janice Caruso is the step-daughter of Mr. Goins and a U.S. national. Janice Caruso lived in the same household as Mr. Goins for a substantial time and considered Mr. Goins the functional equivalent of a biological father.

1005. Plaintiff Dana Rainey is the step-daughter of Mr. Goins and a U.S. national. Dana Rainey lived in the same household as Mr. Goins for a substantial time and considered Mr. Goins the functional equivalent of a biological father.

1006. As a result of the February 10, 2014 IED Attack, and Mr. Goins's injuries and death, each member of the Goins Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. Goins's society, companionship, and counsel.

1007. As a result of the February 10, 2014 IED Attack, Mr. Goins was injured in his person and/or property. The Plaintiff members of the Goins Family are the survivors and/or heirs of Mr. Goins and are entitled to recover for the damages Mr. Goins sustained.

2. The Michael A. Hughes Family

1008. Mr. Michael A. Hughes served in Afghanistan as a civilian government contractor working for DynCorp, Int'l. Mr. Hughes was injured in the February 10, 2014 IED Attack. Mr. Hughes died on February 10, 2014 as a result of injuries sustained during the attack.

1009. Mr. Hughes was a U.S. national at the time of the February 10, 2014 IED Attack and his death.

1010. Plaintiff Kathleen Alexander is the sister of Mr. Hughes and a U.S. national.

1011. Plaintiff Daniel Hughes is the brother of Mr. Hughes and a U.S. national.

1012. Plaintiff Patricia Hughes is the sister of Mr. Hughes and a U.S. national.

1013. Plaintiff Kristine Zitny is the sister of Mr. Hughes and a U.S. national.

1014. As a result of the February 10, 2014 IED Attack, and Mr. Hughes's injuries and death, each member of the Hughes Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Hughes's society, companionship, and counsel.

1015. As a result of the February 10, 2014 IED Attack, Mr. Hughes was injured in his person and/or property. The Plaintiff members of the Hughes Family are the survivors and/or heirs of Mr. Hughes and are entitled to recover for the damages Mr. Hughes sustained.

ZZ. February 15, 2014 Attack In Helmand (Aaron C. Torian Family)

1016. 2424. Master Sergeant Aaron C. Torian served in Afghanistan as a member of the U.S. Marine Corps. On February 15, 2014, MSgt Torian was injured in an IED attack in Helmand ("February 15, 2014 IED Attack"). MSgt Torian died on February 15, 2014 as a result of injuries sustained during the February 15, 2014 IED Attack.

1017. The February 15, 2014 IED Attack was committed by the Taliban.

1018. On information and belief, the bomb that the Taliban detonated during the February 15, 2014 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban's attack.

1019. The February 15, 2014 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who planted the IED neither wore uniforms nor otherwise identified themselves as enemy combatants, and the passive detonation system indiscriminately placed civilians at risk.

1020. MSgt Torian was a U.S. national at the time of the February 15, 2014 IED Attack and his death.

1021. Plaintiff Joe Torian is the father of MSgt Torian and a U.S. national.

1022. Plaintiff Emily Torian is the sister of MSgt Torian and a U.S. national.

1023. As a result of the February 15, 2014 IED Attack, and MSgt Torian's injuries and death, each member of the Torian Family has experienced severe mental anguish, emotional pain and suffering, and the loss of MSgt Torian's society, companionship, and counsel.

1024. As a result of the February 15, 2014 IED Attack, MSgt Torian was injured in his person and/or property. The Plaintiff members of the Torian Family are the survivors and/or heirs of MSgt Torian and are entitled to recover for the damages MSgt Torian sustained.

AAA. August 12, 2014 Attack In Kandahar (Alberto Diaz Family)

1025. Specialist Alberto Diaz served in Afghanistan as a member of the U.S. Army. On August 12, 2014, SPC Diaz was injured in an IED attack in Kandahar ("August 12, 2014 IED

Attack”). The August 12, 2014 IED Attack severely wounded SPC Diaz, who suffered severe brain injuries and facial damage requiring complete right-side facial reconstruction, and also suffers from post-traumatic stress disorder, chronic fatigue syndrome, chronic pain, social anxiety, panic attacks, hearing loss and tremors. As a result of the August 12, 2014 IED Attack and his injuries, SPC Diaz has experienced severe physical and emotional pain and suffering.

1026. The August 12, 2014 IED Attack was committed by the Taliban.

1027. On information and belief, the bomb that the Taliban detonated during the August 12, 2014 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban’s attack.

1028. The August 12, 2014 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants and the passive detonation system indiscriminately placed civilians at risk.

1029. SPC Diaz was a U.S. national at the time of the attack and remains so today.

1030. Plaintiff Kayla Diaz is the wife of SPC Diaz and a U.S. national.

1031. Plaintiff N.J.D., by and through her next friend Kayla Diaz, is the minor daughter of SPC Diaz and a U.S. national.

1032. Plaintiff N.J.A.D., by and through his next friend Kayla Diaz, is the minor son of SPC Diaz and a U.S. national.

1033. Plaintiff Frances Diaz is the mother of SPC Diaz and a U.S. national.

1034. Plaintiff Maximo Diaz is the father of SPC Diaz and a U.S. national.

1035. Plaintiff Anthony Diaz is the brother of SPC Diaz and a U.S. national.

1036. Plaintiff Matthew Diaz is the brother of SPC Diaz and a U.S. national.

1037. As a result of the August 12, 2014 IED Attack and SPC Diaz's injuries, each member of the Diaz Family has experienced severe mental anguish, emotional pain and suffering.

BBB. November 24, 2014 Attack In Kabul (Joseph Riley Family)

1038. Specialist Joseph Riley served in Afghanistan as a member of the U.S. Army. On November 24, 2014, SPC Riley was injured in a vehicle-borne suicide IED attack in Kabul ("November 24, 2014 Suicide Attack"). SPC Riley died on November 24, 2014 as a result of injuries sustained during the November 24, 2014 IED Attack.

1039. The November 24, 2014 Suicide Attack was committed by the Taliban (including its Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

1040. The November 24, 2014 Suicide Attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Kabul Attack Network's funding, logistics, personnel, and weapons supply in his capacity as a member of al-Qaeda's military council, and helped choose the general time and target for the attack.

1041. On information and belief, the suicide bomber who detonated the vehicle borne IED during the November 24, 2014 Suicide Attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to

Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

1042. On information and belief, the device that the suicide bomber detonated during the November 24, 2014 Suicide Attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

1043. The November 24, 2014 Suicide Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants and the detonation of a vehicle indiscriminately placed civilians at risk.

1044. SPC Riley was a U.S. national at the time of the November 24, 2014 Suicide Attack and his death.

1045. Plaintiff Michelle Riley is the mother of SPC Riley and a U.S. national.

1046. Plaintiff Rodney Riley is the father of SPC Riley and a U.S. national.

1047. As a result of the November 24, 2014 Suicide Attack, and SPC Riley's injuries and death, each member of the Riley Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Riley's society, companionship, and counsel.

1048. As a result of the November 24, 2014 Suicide Attack, SPC Riley was injured in his person and/or property. The Plaintiff members of the Riley Family are the survivors and/or heirs of SPC Riley and are entitled to recover for the damages SPC Riley sustained.

CCC. December 12, 2014 Attack In Parwan (Wyatt J. Martin Family)

1049. Specialist Wyatt J. Martin served in Afghanistan as a member of the U.S. Army. On December 12, 2014, SPC Martin was injured in an IED attack in Parwan (“December 12, 2014 IED Attack”). SPC Martin died on December 12, 2014 as a result of injuries sustained during the December 12, 2014 IED Attack.

1050. The December 12, 2014 IED Attack was committed by the Taliban.

1051. On information and belief, the bomb that the Taliban detonated during the December 12, 2014 IED Attack was: (i) based on a signature al-Qaeda IED design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda’s IED manufacturing sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were “cooked” by al-Qaeda chemists; and (iv) provided to the Taliban by al-Qaeda operatives in order to facilitate the Taliban’s attack.

1052. The December 12, 2014 IED Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1053. SPC Martin was a U.S. national at the time of the December 12, 2014 IED Attack and his death.

1054. Plaintiff Julie Martin is the mother of SPC Martin and a U.S. national.

1055. Plaintiff Brian Martin is the father of SPC Martin and a U.S. national.

1056. Plaintiff Catherine Martin is the sister of SPC Martin and a U.S. national.

1057. Plaintiff Elizabeth Martin is the sister of SPC Martin and a U.S. national.

1058. As a result of the December 12, 2014 IED Attack, and SPC Martin’s injuries and death, each member of the Martin Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Martin’s society, companionship, and counsel.

1059. As a result of the December 12, 2014 IED Attack, SPC Martin was injured in his person and/or property. The Plaintiff members of the Martin Family are the survivors and/or heirs of SPC Martin and are entitled to recover for the damages SPC Martin sustained.

DDD. January 29, 2015 Attack In Kabul (Jason D. Landphair Family)

1060. Mr. Jason D. Landphair served in Afghanistan as a civilian government contractor working for Praetorian Standard Inc. On January 29, 2015, Mr. Landphair was injured in an insider attack in Kabul (“January 29, 2015 Insider Attack”). Mr. Landphair died on January 29, 2015 as a result of injuries sustained during the attack.

1061. The January 29, 2015 Insider Attack was committed by the Taliban (including its Haqqani Network), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO) acting together as a joint cell, led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, in the Kabul Attack Network.

1062. The January 29, 2015 Insider Attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Kabul Attack Network’s funding, logistics, personnel, and weapons supply in his capacity as a member of al-Qaeda’s military council, and helped choose the general time and target for the attack.

1063. The January 29, 2015 Insider Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1064. Mr. Landphair was a U.S. national at the time of the January 29, 2015 Insider Attack and his death.

1065. Plaintiff Jean Landphair is the mother of Mr. Landphair and a U.S. national.

1066. Plaintiff Douglas Landphair is the father of Mr. Landphair and a U.S. national.

1067. Plaintiff Meredith Landphair is the sister of Mr. Landphair and a U.S. national.

1068. As a result of the January 29, 2015 Insider Attack, and Mr. Landphair's injuries and death, each member of the Landphair Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. Landphair's society, companionship, and counsel.

1069. As a result of the January 29, 2015 Insider Attack, Mr. Landphair was injured in his person and/or property. The Plaintiff members of the Landphair Family are the survivors and/or heirs of Mr. Landphair and are entitled to recover for the damages Mr. Landphair sustained.

EEE. August 22, 2015 Attack In Kabul (Families Of Corey J. Dodge, Richard P. McEvoy, And Barry Sutton)

1070. On August 22, 2015, a joint cell comprised of the Taliban (including its Haqqani Network, a designated FTO at the time of the attack), al-Qaeda (an FTO), and Lashkar-e-Taiba (an FTO), led by dual-hatted al-Qaeda/Taliban terrorist Ahmed Jan Wazir, and acting together as part of the Kabul Attack Network, committed a suicide bomb attack targeting Americans in Kabul ("August 22, 2015 Suicide Attack").

1071. The August 22, 2015 Suicide Attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Kabul Attack Network's funding, logistics, personnel, and weapons supply in his capacity as a member of al-Qaeda's military council, and helped choose the general time and target for the attack.

1072. On information and belief, the suicide bomber who detonated the bomb during the August 22, 2015 Suicide Attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's

tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

1073. On information and belief, the device that the suicide bomber detonated during the August 22, 2015 Suicide Attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

1074. The August 22, 2015 Suicide Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the targets were civilians not taking part in hostilities, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk, killing multiple Afghan civilians, because it occurred on a public road in front of a private hospital.

1. The Corey J. Dodge Family

1075. Mr. Corey J. Dodge served in Afghanistan as a civilian government contractor working for DynCorp Free Zone. Mr. Dodge was injured in the August 22, 2015 Suicide Attack. Mr. Dodge died on August 22, 2015 as a result of injuries sustained during the attack.

1076. Mr. Dodge was a U.S. national at the time of the August 22, 2015 Suicide Attack and his death.

1077. Plaintiff Kelli Dodge is the widow of Mr. Dodge and a U.S. national.

1078. Plaintiff B.C.D., by and through his next friend Kelli Dodge, is the minor son of Mr. Dodge and a U.S. national.

1079. Plaintiff P.A.D., by and through her next friend Kelli Dodge, is the minor daughter of Mr. Dodge and a U.S. national.

1080. As a result of the August 22, 2015 Suicide Attack, and Mr. Dodge's injuries and death, each member of the Dodge Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. Dodge's society, companionship, and counsel.

1081. As a result of the August 22, 2015 Suicide Attack, Mr. Dodge was injured in his person and/or property. The Plaintiff members of the Dodge Family are the survivors and/or heirs of Mr. Dodge and are entitled to recover for the damages Mr. Dodge sustained.

2. The Richard P. McEvoy Family

1082. Mr. Richard P. McEvoy served in Afghanistan as a civilian government contractor working for DynCorp, Int'l. Mr. McEvoy was injured in the August 22, 2015 Suicide Attack. Mr. McEvoy died on August 22, 2015 as a result of injuries sustained during the attack.

1083. Mr. McEvoy was a U.S. national at the time of the August 22, 2015 Suicide Attack and his death.

1084. Plaintiff Kathleen McEvoy is the widow of Mr. McEvoy and a U.S. national.

1085. Plaintiff Michelle McEvoy is the daughter of Mr. McEvoy and a U.S. national.

1086. Plaintiff Patrick McEvoy is the son of Mr. McEvoy and a U.S. national.

1087. Plaintiff Janice Proctor is the mother of Mr. McEvoy and a U.S. national.

1088. Plaintiff Luann Varney is the sister of Mr. McEvoy and a U.S. national

1089. As a result of the August 22, 2015 Suicide Attack, and Mr. McEvoy's injuries and death, each member of the McEvoy Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. McEvoy's society, companionship, and counsel.

1090. As a result of the August 22, 2015 Suicide Attack, Mr. McEvoy was injured in his person and/or property. The Plaintiff members of the McEvoy Family are the survivors and/or heirs of Mr. McEvoy and are entitled to recover for the damages Mr. McEvoy sustained.

3. The Barry Sutton Family

1091. Mr. Corey J. Dodge served in Afghanistan as a civilian government contractor working for DynCorp Free Zone. Mr. Sutton was injured in the August 22, 2015 Suicide Attack. Mr. Sutton died on August 22, 2015 as a result of injuries sustained during the attack.

1092. Mr. Sutton was a U.S. national at the time of the August 22, 2015 Suicide Attack and his death.

1093. Plaintiff Harriet Sutton is the mother of Mr. Sutton and a U.S. national.

1094. Plaintiff Erin Goss is the daughter of Mr. Sutton and a U.S. national.

1095. Plaintiff Summer Sutton is the daughter of Mr. Sutton and a U.S. national.

1096. Plaintiff Trecia Hood is the sister of Mr. Sutton and a U.S. national.

1097. Plaintiff Wendy Shedd is the sister of Mr. Sutton and a U.S. national.

1098. Plaintiff Freddie Sutton is the brother of Mr. Sutton and a U.S. national.

1099. As a result of the August 22, 2015 Suicide Attack, and Mr. Sutton's injuries and death, each member of the Sutton Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Mr. Sutton's society, companionship, and counsel.

1100. As a result of the August 22, 2015 Suicide Attack, Mr. Sutton was injured in his person and/or property. The Plaintiff members of the Sutton Family are the survivors and/or heirs of Mr. Sutton and are entitled to recover for the damages Mr. Sutton sustained.

FFF. August 26, 2015 Attack In Helmand (Matthew D. Roland Family)

1101. Captain Matthew Roland served in Afghanistan as a member of the U.S. Air Force. On August 26, 2015, Capt Roland was injured in an insider attack in Helmand ("August

26, 2015 Insider Attack”). Capt Roland died on August 26, 2015 as a result of injuries sustained during the attack.

1102. The August 26, 2015 Insider Attack was committed by the Taliban.

1103. The August 26, 2015 Insider Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist who committed the attack was unlawfully wearing the uniform of his enemy.

1104. Capt Roland was a U.S. national at the time of the August 26, 2015 Insider Attack and his death.

1105. Plaintiff Barbara Roland is the mother of Capt Roland and a U.S. national.

1106. Plaintiff Mark Roland is the father of Capt Roland and a U.S. national.

1107. Plaintiff Erica Roland is the sister of Capt Roland and a U.S. national.

1108. As a result of the August 26, 2015 Insider Attack, and Capt Roland’s injuries and death, each member of the Roland Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Capt Roland’s society, companionship, and counsel.

1109. As a result of the August 26, 2015 Insider Attack, Capt Roland was injured in his person and/or property. The Plaintiff members of the Roland Family are the survivors and/or heirs of Capt Roland and are entitled to recover for the damages Capt Roland sustained.

GGG. December 21, 2015 Attack In Parwan (Chester J. McBride III Family)

1110. Staff Sergeant Chester McBride III served in Afghanistan as a member of the U.S. Air Force. On December 21, 2015, SSgt McBride was injured in a suicide bombing attack in Parwan (“December 21, 2015 Suicide Attack”). SSgt McBride died on December 21, 2015 as a result of injuries sustained during the attack.

1111. The December 21, 2015 Suicide Attack was committed by the Taliban and al-Qaeda (an FTO) acting together in a joint al-Qaeda-Taliban cell with al-Qaeda providing and training the suicide bomber.

1112. On information and belief, the suicide bomber who detonated the bomb during the December 21, 2015 Suicide Attack was: (i) indoctrinated by al-Qaeda regarding the purported religious justification that permitted the attack; (ii) trained by al-Qaeda regarding al-Qaeda's tactics, techniques, and procedures for suicide bombers; (iii) deployed by al-Qaeda to Afghanistan in order to attack Americans there; and (iv) a member of al-Qaeda under al-Qaeda training procedures for suicide attackers, as a result of the bomber pledging loyalty to al-Qaeda to create a point of no return.

1113. On information and belief, the device that the suicide bomber detonated during the December 21, 2015 Suicide Attack was: (i) based on a signature al-Qaeda design; (ii) assembled and tested by al-Qaeda bombmakers at one of al-Qaeda's bombmaking sites managed and funded by al-Qaeda/Taliban terrorist Sirajuddin Haqqani; (iii) designed to detonate precursor ingredients that were "cooked" by al-Qaeda chemists; and (iv) provided to the joint cell by al-Qaeda operatives in order to facilitate the joint cell's attack.

1114. The December 21, 2015 Suicide Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1115. SSgt McBride was a U.S. national at the time of the December 21, 2015 Suicide Attack and his death.

1116. Plaintiff Annie McBride is the mother of SSgt McBride and a U.S. national.

1117. Plaintiff Chester McBride Sr. is the father of SSgt McBride and a U.S. national.

1118. As a result of the December 21, 2015 Suicide Attack, and SSgt McBride's injuries and death, each member of the McBride Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSgt McBride's society, companionship, and counsel.

1119. As a result of the December 21, 2015 Suicide Attack, SSgt McBride was injured in his person and/or property. The Plaintiff members of the McBride Family are the survivors and/or heirs of SSgt McBride and are entitled to recover for the damages SSgt McBride sustained.

HHH. January 5, 2016 Attack In Helmand (Matthew Q. McClintock Family)

1120. Sergeant First Class Matthew Q. McClintock served in Afghanistan as a member of the U.S. Army National Guard. On January 5, 2016, SFC McClintock was injured in a complex attack involving small arms fire in Helmand ("January 5, 2016 Complex Attack"). SFC McClintock died on January 5, 2016 as a result of injuries sustained during the attack.

1121. The January 5, 2016 Complex Attack was committed by the Taliban.

1122. The January 5, 2016 Complex Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1123. SFC McClintock was a U.S. national at the time of the January 5, 2016 Complex Attack and his death.

1124. Plaintiff Alexandra McClintock is the widow of SFC McClintock and a U.S. national.

1125. Plaintiff D.C.M. by and through his next friend Alexandra McClintock, is the minor son of SFC McClintock and a U.S. national.

1126. Plaintiff Joyce Paulsen is the mother of SFC McClintock and a U.S. national.

1127. Plaintiff George McClintock III is the father of SFC McClintock and a U.S. national.

1128. As a result of the January 5, 2016 Complex Attack, and SFC McClintock's injuries and death, each member of the McClintock Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SFC McClintock's society, companionship, and counsel.

1129. As a result of the January 5, 2016 Complex Attack, SFC McClintock was injured in his person and/or property. The Plaintiff members of the McClintock Family are the survivors and/or heirs of SFC McClintock and are entitled to recover for the damages SFC McClintock sustained.

III. August 7, 2016 Attack In Kabul (Kevin King Family)

1130. Plaintiff Mr. Kevin King served in Afghanistan as a civilian professor teaching at American University of AFG. On August 7, 2016, Mr. King was kidnapped at gunpoint just outside the front gates of American University of Afghanistan. Mr. King was held hostage under deplorable conditions, beaten frequently, and denied adequate medical care for over three years before being released in a prisoner exchange on November 19, 2019. The attack severely wounded Mr. King, and he has suffered from severe caloric malnutrition, muscle atrophy, peripheral neuropathy, hypocalcemia, vitamin D deficiency, low bone mineral density, hyperparathyroidism, frostbite on feet and ankles, a weak bladder, and other physical injuries due to repeated beatings. As a result of the August 7, 2016 attack and his injuries, Mr. King has experienced severe physical and emotional pain and suffering.

1131. The attack was committed by the Haqqani Network, a designated FTO at the time of the attack and part of the Taliban.

1132. On information and belief, the attack was planned by al-Qaeda (an FTO), including, but not limited to, dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani, who personally coordinated the Syndicate's kidnapping operations in his capacity as a member of al-Qaeda's military council, and helped choose the general time and target for the attack. Among other motivations, Sirajuddin Haqqani sought to kidnap Americans so that he would have a hostage to trade for key Haqqani Network leaders who were in U.S. custody, including, but not limited to, one or more members of the Haqqani family.

1133. The attack that injured Mr. King would have violated the laws of war if these terrorists were subject to them because, among other reasons, he was a civilian college professor not taking part in hostilities and was tortured during captivity, and the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1134. Mr. King was a U.S. national at the time of the attack and remains so today.

1135. Plaintiff Stephanie Miller is the sister of Mr. King and a U.S. national.

1136. As a result of the August 7, 2016 attack and Mr. King's injuries, each member of the King Family has experienced severe mental anguish, emotional pain and suffering.

JJJ. The June 10, 2017 Attack In Nangarhar (Families of William M. Bays and Dillon C. Baldrige)

1137. On June 10, 2017, al-Qaeda (an FTO), the Taliban, and Lashkar-e-Taiba (an FTO), acting together in a joint cell committed an insider attack targeting Americans in Nangarhar ("June 10, 2017 Insider Attack").

1138. The June 10, 2017 Insider Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack was lawfully wearing the uniform of his enemy.

1. The William M. Bays Family

1139. Sergeant William M. Bays served in Afghanistan as a member of the U.S. Army. SGT Bays was injured in the June 10, 2017 Insider Attack. SGT Bays died on June 10, 2017 as a result of injuries sustained during this attack.

1140. SGT Bays was a U.S. national at the time of the attack and his death.

1141. Plaintiff Timothy Bays is the father of SGT Bays and a U.S. national.

1142. Plaintiff April Bays is the mother of SGT Bays and a U.S. national.

1143. Plaintiff Lindsay Bays is the sister of SGT Bays and a U.S. national.

1144. Plaintiff Brenda Griner is the sister of SGT Bays and a U.S. national.

1145. Plaintiff Jasmin Bays is the widow of SGT Bays and a U.S. national.

1146. Plaintiff Julia Steiner is the step-daughter of SGT Bays and a U.S. national. Julia Steiner lived in the same household as SGT Bays for a substantial time and considered SGT Bays the functional equivalent of a biological father.

1147. Plaintiff L.S., by and through her next friend Jasmin Bays, is the minor step-daughter of SGT Bays and a U.S. national. L.S. lived in the same household as SGT Bays for a substantial time and considered SGT Bays the functional equivalent of a biological father.

1148. Plaintiff M.S., by and through her next friend Jasmin Bays, is the minor step-daughter of SGT Bays and a U.S. national. M.S. lived in the same household as SGT Bays for a substantial time and considered SGT Bays the functional equivalent of a biological father.

1149. As a result of the June 10, 2017 Insider Attack, and SGT Bays's injuries and death, each member of the Bays Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Bays's society, companionship, and counsel.

1150. As a result of the June 10, 2017 Insider Attack, SGT Bays was injured in his person and/or property. The Plaintiff members of the Bays Family are the survivors and/or heirs of SGT Bays and are entitled to recover for the damages SGT Bays sustained.

2. The Dillon C. Baldrige Family

1151. Sergeant Dillon C. Baldrige served in Afghanistan as a member of the U.S. Army. SGT Baldrige was injured in the June 10, 2017 Insider Attack. SGT Baldrige died on June 10, 2017 as a result of injuries sustained during this attack.

1152. SGT Baldrige was a U.S. national at the time of the attack and his death.

1153. Plaintiff Christopher Baldrige is the father of SGT Baldrige and a U.S. national.

1154. Plaintiff S.B., by and through her next friend Christopher Baldrige, is the minor sister of SGT Baldrige and a U.S. national.

1155. Plaintiff L.B., by and through his next friend Christopher Baldrige, is the minor brother of SGT Baldrige and a U.S. national.

1156. Plaintiff E.B., by and through his next friend Christopher Baldrige, is the minor brother of SGT Baldrige and a U.S. national.

1157. As a result of the June 10, 2017 Insider Attack, and SGT Baldrige's injuries and death, each member of the Baldrige Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Baldrige's society, companionship, and counsel.

1158. As a result of the June 10, 2017 Insider Attack, SGT Baldrige was injured in his person and/or property. The Plaintiff members of the Baldrige Family are the survivors and/or heirs of SGT Baldrige and are entitled to recover for the damages SGT Baldrige sustained.

KKK. July 3, 2017 Fire Attack In Helmand (Hansen B. Kirkpatrick Family)

1159. Private First Class Hansen B. Kirkpatrick served in Afghanistan as a member of the U.S. Army. On July 3, 2017, PFC Kirkpatrick was injured in an indirect fire attack in

Helmand (“July 3, 2017 Indirect Fire Attack”). PFC Kirkpatrick died on June 18, 2013 as a result of injuries sustained during the July 3, 2017 Indirect Fire Attack.

1160. The July 3, 2017 Indirect Fire Attack was committed by the Taliban.

1161. The July 3, 2017 Indirect Fire Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants.

1162. PFC Kirkpatrick was a U.S. national at the time of the attack and his death.

1163. Plaintiff Anngel Norkist is the mother of PFC Kirkpatrick and a U.S. national.

1164. Plaintiff Aujza Norkist is the sister of PFC Kirkpatrick and a U.S. national.

1165. Plaintiff Hart Norkist is the brother of PFC Kirkpatrick and a U.S. national.

1166. Plaintiff William Newnham is the step-father of PFC Kirkpatrick and a U.S. national. William Newnham lived in the same household as PFC Kirkpatrick for a substantial period of time and considered PFC Kirkpatrick the functional equivalent of a biological son.

1167. As a result of the July 3, 2017 Indirect Fire Attack, and PFC Kirkpatrick’s injuries and death, each member of the Kirkpatrick Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC Kirkpatrick’s society, companionship, and counsel.

1168. As a result of the July 3, 2017 Indirect Fire Attack, PFC Kirkpatrick was injured in his person and/or property. The Plaintiff members of the Kirkpatrick Family are the survivors and/or heirs of PFC Kirkpatrick and are entitled to recover for the damages PFC Kirkpatrick sustained.

CLAIMS FOR RELIEF

COUNT ONE: VIOLATION OF THE ANTI-TERRORISM ACT, 18 U.S.C. § 2333(d) **[All Defendants: Aiding-And-Abetting Liability, Attack Predicate]**

1169. Plaintiffs incorporate their factual allegations above.

1170. The terrorist attacks that killed or injured Plaintiffs or their family members were acts of international terrorism against Americans in Afghanistan committed by: (i) joint cells comprised of al-Qaeda, a designated FTO at all times and the Taliban,⁵⁹⁶ a designated SDGT at all times, including its Haqqani Network, a designated SDGT after 2001 and a designated FTO after September 19, 2012, with the material support of the IRGC,⁵⁹⁷ including Hezbollah, a designated FTO at all times, and the Qods Force, a designated SDGT after October 25, 2007, which attacks were committed, planned, and/or authorized by al-Qaeda, a designated FTO at all times; or (ii) the Taliban, a designated SDGT at all times, including its Haqqani Network, a designated SDGT after 2001 and a designated FTO after September 19, 2012, with the material support of the IRGC, including Hezbollah, a designated FTO at all times, and the Qods Force, a designated SDGT after October 25, 2007, which attacks were committed, planned, and/or authorized by al-Qaeda, a designated FTO at all times.

1171. The terrorist attacks committed by al-Qaeda and/or the Taliban, including its Haqqani Network with the material support of the IRGC, which killed or injured Plaintiffs and their family members, were violent acts and acts dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the jurisdiction of the United States or of the States. In particular, each

⁵⁹⁶ In each Count in this Complaint, any reference to “Taliban” is inclusive of the Haqqani Network, which is a part of the Taliban.

⁵⁹⁷ In each Count in this Complaint, any reference to “IRGC” is inclusive of Hezbollah, the Qods Force, and Regular IRGC, all of which are constituent parts of the IRGC.

attack constituted one or more of murder, attempted murder, conspiracy to murder, kidnapping, and arson, in violation of state law; and the destruction of U.S. property by fire or explosive, conspiracy to murder in a foreign country, killing and attempted killing of U.S. employees performing official duties, hostage taking, damaging U.S. government property, killing U.S. nationals abroad, use of weapons of mass destruction, commission of acts of terrorism transcending national boundaries, and bombing places of public use, in violation of 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, and 2332f, respectively.

1172. The terrorist attacks committed by al-Qaeda and/or the Taliban, including its Haqqani Network, with the material support of the IRGC appear to have been intended (a) to intimidate or coerce the civilian populations of Afghanistan, the United States, and other Coalition nations, (b) to influence the policy of the U.S., Afghan, and other Coalition governments by intimidation and coercion, and (c) to affect the conduct of the U.S., Afghan, and other Coalition governments by mass destruction, assassination, and kidnapping.

1173. The terrorist attacks committed by al-Qaeda and/or the Taliban, including its Haqqani Network, with the material support of the IRGC occurred primarily outside the territorial jurisdiction of the United States.

1174. Each of ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC al-Qaeda, and the Taliban, including its Haqqani Network – and aided and abetted and knowingly provided substantial assistance to the al-Qaeda and/or Taliban attacks on Plaintiffs – by providing funds to known IRGC fronts and technical support to Hezbollah, the Qods Force, and Regular IRGC that aided those attacks, and

by making protection payments to the Taliban, including its Haqqani Network, in both cash and “free goods.”

1175. ZTE and Huawei also aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC – and aided and abetted and knowingly provided substantial assistance to the IRGC’s proxy attacks on Plaintiffs committed by al-Qaeda and/or the Taliban – by serving as the joint venture partner of Hezbollah, the Qods Force, and Regular IRGC and generating millions of dollars in annual cash flow for Hezbollah, the Qods Force, and Regular IRGC to use in furtherance of the IRGC’s support for proxy attacks by al-Qaeda and/or the Taliban, including its Haqqani Network, against Americans in Afghanistan.

1176. ZTE, including but not limited to in coordination with ZTE USA and ZTE TX, aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC – and aided and abetted and knowingly provided substantial assistance to the IRGC’s proxy attacks on Plaintiffs committed by al-Qaeda and/or the Taliban – by contracting with TCI to modernize the IRGC-controlled Iranian cellular and landline communications systems, thereby generating substantial revenue for Hezbollah, the Qods Force, and Regular IRGC and provided U.S.-origin technology to the IRGC, which the IRGC flowed through to al-Qaeda and the Taliban, including its Haqqani Network, all of which al-Qaeda and the Taliban, including its Haqqani Network, used in furtherance of al-Qaeda’s and the Taliban’s, including the Haqqani Network’s, shared terrorist enterprise against Americans in Afghanistan.

1177. Huawei, including but not limited to and in coordination with Skycom, Huawei USA, Huawei Device USA, and Futurewei, aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, and Regular IRGC – and aided and abetted

and knowingly provided substantial assistance to the IRGC's proxy attacks on Plaintiffs committed by al-Qaeda and/or the Taliban – by contracting with TCI to modernize the IRGC-controlled Iranian cellular and landline communications systems, thereby generating substantial revenue for Hezbollah, the Qods Force, and Regular IRGC and illegally provided U.S.-origin technology to Hezbollah, the Qods Force, and Regular IRGC, which the IRGC flowed through to al-Qaeda and the Taliban, including its Haqqani Network, all of which al-Qaeda and the Taliban, including its Haqqani Network, used in furtherance of al-Qaeda's and the Taliban's, including the Haqqani Network's, shared terrorist enterprise against Americans in Afghanistan.

1178. The attacks that killed or injured Plaintiffs and their family members were all jointly committed, as well as planned and authorized, by al-Qaeda, which the United States has designated as an FTO under 8 U.S.C. § 1189 since 1999.

1179. Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by al-Qaeda and/or the Taliban. Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1180. As a result of Defendants' liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

COUNT TWO: VIOLATION OF THE ANTI-TERRORISM ACT, 18 U.S.C. § 2333(d)
[All Defendants: Conspiracy Liability; Attack Predicate]

1181. Plaintiffs incorporate their factual allegations above.

1182. Each of ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom entered into a conspiracy with the "Iranian Shareholders," and one another, including but not limited to the Bonyad Mostazafan, MTN Irancell, MTN Group, MTN Dubai, IEI, TCI (including MCI), and Exit40, all of whom were fronts for the

IRGC (collectively, “IRGC Fronts”), including its Hezbollah Division and Qods Force, as well as the IRGC’s terrorist co-conspirators in Afghanistan, al-Qaeda and the Taliban (including its Haqqani Network), to join the IRGC’s terrorist financing and logistics campaign.

1183. Each of ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom each furthered the conspiracy through their knowing direct and/or indirect participation in the IRGC’s broad, coordinated, global campaign to source embargoed American technologies to aid the conspiracy’s terrorist enterprise, including but not limited to, secure American mobile phones and computer network technologies.

1184. Given the illegal nature of the illicit market for purchasing embargoed American technologies, each Defendant’s choice to further the conspiracy by paying inflated prices above even the normal “going rate” for black market phones furthered the terrorist enterprise by substantially growing the black market for such technologies through the power of supply and demand. Every time each Defendant flooded the zone by promising to outspend every other black-market participant, Defendants swelled the ranks of their co-conspirator tech resellers on the supply side in the U.S.

1185. Each of ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom specifically intended to grow the overall global market for illicit American-manufactured mobile phones that were originally sold in a U.S. marketplace because they shared the goal of the conspiracy, which was to finance, arm, and logistically support Hezbollah, the Qods Force, and Regular IRGC.

1186. Each of ZTE Corp., ZTE USA, ZTE TX, Huawei Co., Huawei USA, Huawei Device USA, Futurewei, and Skycom were one in spirit with the terrorists, including, but not limited to, Hezbollah, the Qods Force, and Regular IRGC al-Qaeda, the Taliban, including its

Haqqani Network, all of whom were proxies of the IRGC and all of whom received weapons, funding, and training from the IRGC.

1187. Each Defendant hoped for the IRGC, including, but not limited to, its Hezbollah Division and Qods Force, to achieve the object of the conspiracy and force the United States to withdraw from Afghanistan, Iraq, and the rest of the Middle East. Defendants knew that Hezbollah, the Qods Force, and Regular IRGC were extremely lucrative customers and generated billions of dollars in profits for each Defendant, and Defendants wanted to see the conspiracy succeed because they calculated they would make more money if the terrorist campaigns in Afghanistan, Iraq, and the rest of the Middle East forced the U.S. out.

1188. Defendants ZTE and Huawei also supported the object of the conspiracy because it furthered the hostile security strategy of the Chinese Communist Party to force the United States out of Iraq, Afghanistan, and the rest of the Middle East by aiding the terrorist groups targeting Americans throughout the region.

1189. Each Defendant furthered the conspiracy by directly aiding the growth of the terrorists' supply chain through the foreseeable, inevitable, and obvious result that Defendants knew – and intended – would occur when they paid above-black-market prices for illicit American technologies. Defendants knew that their transactions would strengthen the terrorists' illicit technological supply chain by exploding the demand for suppliers, and specifically intended for this consequence to occur to the benefit Hezbollah, the Qods Force, and Regular IRGC. As a result, each Defendant furthered the conspiracy by increasing the total volume of illicit American mobile phones and computer network technologies specifically available for, and intended to be purchased by, the agents, operatives, cut-outs, or corporate fronts acting on behalf of Hezbollah, and the Qods Force, all of whom received substantially more illicit

technologies than would otherwise have been the case if Defendants had not participated in the black market.

1190. Each supplier Defendant – ZTE Corp. and Huawei Co. – furthered the conspiracy by publicly denying the existence of their secret agreement to aid the “security” agenda of the Iranian Shareholders who own MTN Irancell and TCI, i.e., Hezbollah, the Qods Force, and Regular IRGC.

1191. Each manufacturer Defendant – ZTE (USA) Inc., ZTE (TX) Inc., Huawei Technologies Co., Ltd., Huawei Technologies USA Inc., and Huawei Device USA Inc., – furthered the conspiracy by, among other things: (1) knowingly supplying state-of-the-art American technology while knowing that such technology was being transferred pursuant to deals that were designed to flow the technology through to Hezbollah, the Qods Force, and Regular IRGC; and (2) on information and belief, subsidizing the bribes that ZTE Corp. paid to IRGC officials to secure ZTE’s business with the IRGC’s fronts.

1192. ZTE (USA) Inc. and ZTE (TX) Inc. also furthered the conspiracy by successfully interfering with whistleblower activity, which, on information and belief, materially delayed the disclosure of the fraud, and further concealed the scheme, causing substantial additional value to flow to the terrorists.

1193. ZTE (USA) Inc.’s and ZTE (TX) Inc.’s retaliation against one or more whistleblowers was an act in furtherance of the Conspiracy because it was intended to deter future employees, officers, attorneys, or agents of ZTE (USA) Inc. and ZTE (TX) Inc. from alerting authorities about other potential acts that would destroy the effectiveness of the Conspirators to continue to access the ZTE (USA) Inc. and ZTE (TX) Inc. technology upon which they relied.

1194. ZTE, and Huawei agreed to further this conspiracy by assisting the IRGC fronts to move large sums of money (primarily in U.S. dollars) through the international financial system (and particularly the United States) undetected.

1195. ZTE, and Huawei agreed to further this conspiracy by each assisting the IRGC fronts to move tens of thousands of critical items of embargoed American technologies specifically identified by Hezbollah and the Qods Force as necessary to the success of the conspiracy, doing so through the covert purchase of American-made technologies in U.S. markets, in transactions that were denominated in U.S. Dollars, in sums of money (primarily in U.S. dollars) through the international financial system (and particularly the U.S.) undetected.

1196. As explained above, Hezbollah, the Qods Force, and Regular IRGC conspired with proxies in Afghanistan (al-Qaeda and the Taliban, including its Haqqani Network) to facilitate terrorist attacks targeting Americans in Afghanistan and Iraq, among other places, for the purpose of targeting U.S. citizens and institutions and affecting the policies of the U.S. government.

1197. Each Defendant knew that the objective of the IRGC Conspiracy between these sophisticated terrorist organizations and the other Defendants was to facilitate terrorist attacks against Americans in Afghanistan, Iraq, Syria, Yemen, Israel, and Europe. This includes the attacks at issue in this case that were planned, authorized, or executed by designated FTOs.

1198. These attacks were a foreseeable act in furtherance of this IRGC conspiracy that caused Plaintiffs' injuries.

1199. The attacks that killed or injured Plaintiffs and their family members were all jointly committed, as well as planned and authorized, by al-Qaeda, which the United States has designated as an FTO under 8 U.S.C. § 1189 since 1999.

1200. Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by al-Qaeda and/or the Taliban. Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1201. As a result of Defendants' liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

COUNT THREE: VIOLATION OF THE ANTI-TERRORISM ACT, 18 U.S.C. § 2333(d)
[All Defendants: Aiding-and-Abetting Liability, RICO predicate]

1202. Plaintiffs incorporate their factual allegations above.

1203. From at least 2007 through 2017, IRGC terrorists from Hezbollah, the Qods Force, and Regular IRGC, and al-Qaeda conspired with Mullah Omar, Sirajuddin Haqqani, and others to conduct and maintain the Taliban as a terrorist enterprise capable of carrying out sophisticated attacks on American targets in Afghanistan. Throughout that time, the Taliban was a group of associated individuals that functioned as a continuing unit, and the Taliban's express purpose at all times included violence against, and the expulsion of, Americans in Afghanistan. The Taliban engaged in, and its activities affected, foreign commerce.

1204. From at least 2007 through 2017, the IRGC, Mullah Omar, Sirajuddin Haqqani and other terrorists employed by or associated with the Taliban and al-Qaeda (including, without limitation, Jalaluddin Haqqani and other terrorists described in this Complaint) have maintained interests in and conducted the affairs of the Taliban as an enterprise by engaging in a campaign to expel Americans from Afghanistan through crime and anti-American violence (the "IRGC-Taliban-al-Qaeda Campaign").

1205. Specifically, Mullah Omar, Sirajuddin Haqqani, and other terrorists employed by or associated with the Taliban and al-Qaeda conducted and participated in the conduct of the

Taliban's affairs (and conspired to do so) through a pattern of racketeering activity involving crimes that include murder, attempted murder, conspiracy to murder, kidnapping, and arson, in violation of state law, and the destruction of U.S. property by fire or explosive, conspiracy to murder in a foreign country, killing and attempted killing U.S. employees performing official duties, hostage taking, damaging U.S. government property, killing U.S. nationals abroad, use of weapons of mass destruction, commission of acts of terrorism transcending national boundaries, bombing places of public use, financing terrorism, and receiving training from an FTO, in violation of 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2332f, 2339C(a)(1)(B), and 2339D, respectively. The same terrorists also maintained interests in and control of the Taliban (and conspired to do so) through this pattern of racketeering activity.

1206. The IRGC-Taliban-al-Qaeda Campaign was an act of international terrorism. It was a violent act that was dangerous to human life and that violated the criminal laws of the United States prohibiting the conduct or participation in the conduct of an enterprise's affairs through a pattern of racketeering activity, 18 U.S.C. § 1962(c); the maintenance of an interest in or control of an enterprise through a pattern of racketeering activity, 18 U.S.C. § 1962(b); and conspiring to do either of these acts, 18 U.S.C. § 1962(d); or would have violated these prohibitions had it been conducted within the jurisdiction of the United States. The IRGC-Taliban-al-Qaeda Campaign appears to have been intended (a) to intimidate or coerce the civilian populations of Afghanistan, the United States, and other Coalition nations, (b) to influence the policy of the U.S., Afghan, and other Coalition governments by intimidation and coercion, and (c) to affect the conduct of the U.S., Afghan, and other Coalition governments by mass destruction, assassination, and kidnapping.

1207. The IRGC-Taliban-al-Qaeda Campaign occurred primarily outside the territorial jurisdiction of the United States.

1208. Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the IRGC-Taliban-al-Qaeda Campaign. Specifically, the attacks that injured Plaintiffs were part of the pattern of racketeering activity through which the IRGC, Mullah Omar, Sirajuddin Haqqani, and other terrorists associated with the Taliban and al-Qaeda conducted the affairs of, participated in conducting the affairs of, and maintained an interest in or control of the Taliban. Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the IRGC-Taliban-al-Qaeda Campaign; are the survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1209. Defendants aided and abetted and knowingly provided substantial assistance to Hezbollah, the Qods Force, the Regular IRGC, al-Qaeda, and the Taliban, including its Haqqani Network, which flowed through to the IRGC-Taliban-al-Qaeda Campaign. Defendants did so by making payments to the IRGC that indirectly financed the Taliban's terrorist attacks, and, by authorizing, paying, and/or facilitating millions in annual protection payments to the Taliban, including its Haqqani Network, in cash and "free goods" every year since on or about 2008.

1210. The IRGC-Taliban-al-Qaeda Campaign was committed, planned, and/or authorized by Hezbollah, al-Qaeda, and the Haqqani Network, each of which the United States has designated as an FTO under 8 U.S.C. § 1189 since (in 1997, 1999, and 2012, respectively).

1211. As a result of Defendants' liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

JURY DEMAND

1212. In accordance with Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

1213. Plaintiffs request that the Court:

- (a) Enter judgment against Defendants finding them jointly and severally liable under the Anti-Terrorism Act, 18 U.S.C. § 2333;
- (b) Award Plaintiffs compensatory and punitive damages to the maximum extent permitted by law, and treble any compensatory damages awarded under the Anti-Terrorism Act pursuant to 18 U.S.C. § 2333(a);
- (c) Award Plaintiffs their attorney's fees and costs incurred in this action, pursuant to 18 U.S.C. § 2333(a);
- (d) Award Plaintiffs prejudgment interest; and
- (e) Award Plaintiffs any such further relief the Court deems just and proper.

Dated: April 3, 2022

Respectfully submitted,

/s/ Eli J. Kay-Oliphant

Eli J. Kay-Oliphant (EDNY Bar No. EK8030)

Ryan R. Sparacino (*pro hac vice* pending)

Shuman Sohrn (*pro hac vice* pending)

Sparacino PLLC

1920 L Street, NW, Suite 8358

Washington, D.C. 20036

Tel: (202) 629-3530

ryan.sparacino@sparacinoplhc.com

eli.kay-oliphant@sparacinoplhc.com

Counsel for Plaintiffs